**Introduction** Esta adaptação aplica-se a todas as atividades compreendidas dentro do life-cycle dos sistemas relacionados com a segurança que incluem partes E/E e componentes de software

Assistencia à condução, propulsão, controlo dinâmico, sistemas passivos e ativos gradualmente tocam o domínio dos sistemas relacionados com segurança.

O desenvolvimento e integração destas funcionalidades irão reforçar a necessidade do desenvolvimento de sistemas de segurança e a necessidade de fornecer provas de que todos os objetivos relacionados com a segurança são cumpridos

Com a tendencia do aumento da complexidade tecnologica, conteudo de sw e implementação de mecatronica, há riscos acrescidos de falhas sistematicas e falhas randomicas. ISO 26262 inclui guias para evitar estes riscos fornecendo requisitos e processos apropriados.

A Segurança dos Sistemas é alcançada por meio de metricas de segurança que são implementadas por meio de uma variedade de tecnologias e aplicadas em vários níveis do processo de desenvolvimento. O ISO 26262:

a) fornece um life-cycle de segurança para a industria automóvel (gestão, desenvolvimento, produção, operação, serviço, fim de vida) e dá suporte à adaptação das atividades necessárias ao longo das fases do ciclo de vida.

b) fornece uma abordagem baseada no risco especificamente para a industria automotiva para a determinação de níveis de integridade (ASIL)

c) Usa os ASIL para especificar requisitos aplicáveis do ISO 26262 para evitar riscos residuais não razoáveis

d) fornece requisitos para medidas de validação e confirmação que garantem que um suficiente e aceitável nivel de segurança seja obtido

e) fornece requisitos para a relação com fornecedores (ALTRAN)

Segurança funcional é influenciada pelo processo de desenvolvimento (inclusive atividades como especificação de requisitos , projeto, implementação , integração verificação validação e configuração), pelos processos de produção e serviço e pelos processo de gestão

Questões relacionadas com a segurança estão interligadas com atividades de desenvolvimento orientadas à função, qualidade e work products (Protótipos, apresentações, etc)

A Figura 1 mostra uma visão genérica desta edição do ISO 26262. ISO 26262 baseia-se no modelo em V como referencia. O V representa a interconexão entre os ISOs -3, -4, -5 -6 -7

As cláusulas específicas são indicadas da seguinte forma: “m-n” onde m representa o numero da parte particular e n indica o numero da clausula dentro da parte

**Road vehicles — Functional safety —**

Part 1: **Vocabulary**

Ambito

Pretende-se que o ISO 26262 seja aplicado a sistemas relacionados com segurança que incluam um ou mais sistema E/E e que sejam instalados em veiculos de passageiros em produção em série com massa até 3500 kg. ISO 26262. Não se aplica a veiculos produzidos para pessoas com necessidades especiaisISO 26262 contempla possiveis danos causados pelo mal funcionamento dos sistemas E/E relacionados com segurança incluindo interações com estes sistemas.

ISO 26262 não contempla as performances nominais dos sistemas E/E mesmo que padrões de performance funcionais existam para estes sistemas. (sistemas de segurança ativo e passivo, sistemas de travões, adaptive cruise control)

### **1 Terms and definitions** For the purposes of this document, the following terms and definitions apply.

### 1.1 allocation (Requisito 🡪 Elemento Arquitetural)

Atribuição de um requisito a um elemento arquitetural (1.32)

### Nota: A intenção não é dividir um requisito atomico em multiplos requisitos. (?) Tracing of an atomic **system** (1.129) level requirement to multiple lower level atomic requirements is allowed.

### 1.2 anomaly

Condiçao que diverge do comportamento esperado, por exemplo, divergencia de um requisito, divergencia de uma especificação, divergencia de documentos de projeto, divergencia de padrões ou divergencia de uma prática corrente

### Nota: Anomalias podem ser descobertas, dentre outros intervalos, durante revisões, testes, análises, compilação ou uso de componentes ou documentos aplicáveis.

### 1.3 architecture

### Representação da estrutura de um item ou funções, sistemas, elementos que permita a identificação de blocos de construção, suas fronteiras e interfaces **e incluem allocation (1.1) de funções aos elementos de hw e sw**

### 1.4 assessment

Avaliação de uma característica de um item ou um elemento

### Nota O nível de independencia (1.161) do avaliador que realiza a avaliação está associada a cada avaliação1.5 audit

### Exame de um processo implementado

### 1.6 Automotive Safety Integrity Level ASIL

Um dos 4 níveis (A menos rigoroso e D mais rigoroso) que especificam as medidas de segurança necessárias do ISO 26262 a serem aplicadas aos items ou elementos para que se evite um risco residual não aceitável.

### 1.7 ASIL decomposition

Partiçao de requisitos de segurança de elementos, de redundante para suficientemente independentes com o objetivo de se reduzir o ASIL do requisito de segurança redundantes que estão alocados aos elementos correspondentes.

### 1.8 availability

Capacidade de um produto estar pronto para executar a função requerida em determinadas condições, em um certo tempo ou num determinado período, pressupondo-se que os recursos externos estão disponíveis

### 1.9 baseline

Versão de um conjunto de um ou mais protótipos, items, elements que está sob gestão de configuração e usado como base para posteriores desenvolvimentos através de alterações do processo de gestão

### 1.10 branch coverage

Percentagem dos ramos do fluxo de controlo (do sw) que foram executados

NOTE 1 100 % branch coverage implies 100 % **statement coverage** (1.127).

NOTE 2 An if-statement always has two branches - condition true and condition false - independent of the existence of an else-clause.

### 1.11 calibration data

Dados que serão aplicados após o build do sw no processo de desenvolvimento

EXAMPLE Parameters (e.g. value for low idle speed, engine characteristic diagrams); vehicle specific parameters (adaptation values) (e.g. limit stop for throttle valve); variant coding (e.g. country code, left-hand/right-hand steering).

### Dados de calibração não pode conter código executável ou interpretável

### 1.12 candidate

Item ou elemento cuja definição e condições de uso são identicas a, ou tem um alto grau de identidade com um item ou elemento que já foi disponibilizado e está em operação

NOTA esta definição aplica se onde um candidato é usado no contexto de um argumento de comprovação pelo uso

NOTE This definition applies where candidate is used in the context of a **proven in use argument** (1.90).

### 1.13 cascading failure

**Falha de um elemento de um item que provoca a falha um elemento ou elementos do mesmo item**

**Nota: Cascading Failures são falhas dependentes que não são commom cause failures.**



**Figure 2 — Cascading failure**

### 1.14 common cause failure CCF

**Falha de dois ou mais elementos de um item que resulta de uma falha de um evento simples ou causa raiz;**

NOTE Common cause failures are **dependent failures** (1.22) that are not **cascading failures** (1.13). See Figure 3.

****

**Figure 3 — Common cause failure**

### 1.15 component

Elemento fora do nível do sistema que está logicamente e tecnicamente separável e é composto por mais que uma parte de hw ou uma ou mais unidades de sw

Nota Um componente é uma parte de um sistema.

non-**system** (1.129) level **element** (1.32) that is logically and technically separable and is comprised of more than one **hardware part** (1.55) or of one or more **software units** (1.125)

NOTE A component is a part of a system.

### 1.16 configuration data

Dado que é atribuído ao build do sw e que controla o processo de build

data that is assigned during software build and that controls the software build process

EXAMPLE Pre-processor instructions; software build scripts (e.g. XML configuration files).NOTE 1 Configuration data cannot contain executable or interpretable code.

### NOTE 2 Configuration data controls the software build. Only code, or data selected by configuration data can be included in the executable code.

### 1.17 confirmation measure

**confirmation review** (1.18), **audit** (1.5) or **assessment** (1.4) concerning **functional safety** (1.51)

### 1.18 confirmation review

Confirmação de que um protótipo cumpre os requisitos da ISO 26262 com o requerido nivel de independencia do revisorNOTE 1 A complete list of confirmation reviews is given in ISO 26262-2.

NOTE 2 The goal of confirmation reviews is to ensure compliance with ISO 26262.

|  |  |
| --- | --- |
| 1.19 controllability |  |
| ability to avoid a specified **harm** (1.56) or damage through the timely reactions of the persons involved, possibly with support from **external measures** (1.38) | Capacidade em evitar um determinado dano ou avaria através de reações atempadas das pessoas envolvidas, possivelmente com apoio de medidas externas |
| NOTE 1 Persons involved can include the driver, passengers or persons in the vicinity of the vehicle's exterior. | NOTE 1 Persons involved can include the driver, passengers or persons in the vicinity of the vehicle's exterior. |
| NOTE 2 The parameter C in hazard analysis and risk assessment (1.58) represents the potential for controllability. | NOTE 2 The parameter C in hazard analysis and risk assessment (1.58) represents the potential for controllability. |

### 1.20 dedicated measure

Medida que garante a taxa de falhas declarada na avaliação da probabilidade da violação dos safety goals

EXEMPLO características de projeto; testes sobre amostras de material adquirido para reduzir o risco de ocorrencia failure modes que contribuem para a violação dos safety goals; burn in test; plano de controlo dedicado.

### 1.21 degradation

Estrategia em fornecer safety por projeto após a ocorrencia de failures

Nota Degradação pode incluir funcionalidade reduzida, performance reduzida ou ambos

### 1.22 dependent failures

**Failures cujas probabilidades de ocorrencia simultanea ou sucessiva não pode ser expressa como o simples produto das probabilidades incondicionais de cada uma delas**

NOTE 1 Dependent failures A e B pode ser caracterizado quando *P*AB != *P*A X *P*B

Onde

*P*AB is the probability of the simultaneous occurrence of failure A and failure B;

*P*A is the probability of the occurrence of failure A;

*P*B is the probability of the occurrence of failure B.

NOTE 2 Dependent failures incluem **common cause failures** (1.14) e **cascading failures** (1.13).

### 1.23 detected fault

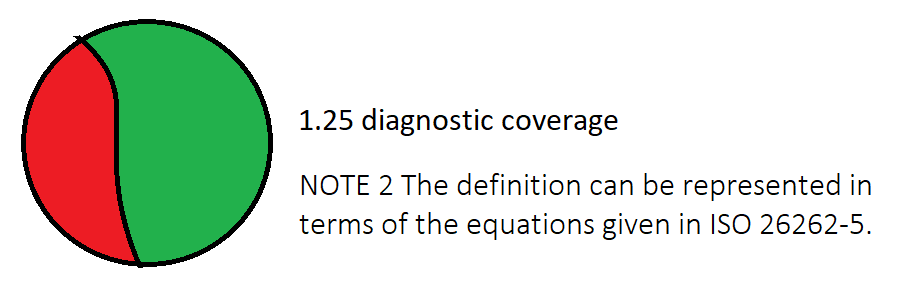
Fault cuja presença é detetada dentro de um tempo predeterminado por um safety mechanism que impede que a falha seja latente

Exemplo A fault pode ser detetada por um mecanismo de safety coinforme definido no functional safety concept

|  |  |
| --- | --- |
| 1.24 development interface agreement **DIA** | **VER COM O PRADO** |
| agreement between customer and supplier in which the responsibilities for activities, evidence or work products to be exchanged by each party are specified  *For instance it is always required to define the responsibilities during product development clearly towards the cus­tomer but also towards the supplier. The corresponding work product in the ISO 26262 is called Development Interface Agreement, DIA in short. A DIA is fun­damentally important for each project related to functional safety and cannot be omitted. (Effects of ISO 26262 on Commercial Vehicle and Steering System)*  *The Development Interface Agreement (DIA) is the single-most important document to ensure successful planning and completion of a program’s Functional Safety goals. It is meant to be a tool and record of what is expected to be completed by each party and should specify the exact means for completion.* <https://www.kvausa.com/development-interface-agreement-the-key-to-a-successful-functional-safety-program/> | Acordo entre consumidor e fornecedor no qual as responsabilidades para atividades, provas ou prototipos a serem trocadas por cada participante são especificadas. |

### 1.25 diagnostic coverage

Proporção do elemento de hardware failure rate que é detetado ou controlado pelo safety mechanism implementado



Nota 1 Diagnostic Coverage pode ser avaliado relativamente ao **residual faults** ou relativamente ao latente **multiple-point faults** que pode ocorrer num elemento de hardware

NOTE 1 Diagnostic coverage can be assessed with regard to **residual faults** (1.96) or with regard to latent **multiple-point faults** (1.77) that might occur in a hardware element.

NOTE 2 The definition can be represented in terms of the equations given in ISO 26262-5.

NOTE 3 Safety mechanisms implemented at different levels in the **architecture** (1.3) can be considered.

### 1.26 diagnostic test interval

Tempo entre execuções de testes de diagnostico online por um safety mechanism

|  |  |
| --- | --- |
| 1.27 distributed development |  |
| development of an **item** (1.69) or **element** (1.32) with development responsibility divided between the customer and supplier(s) for the entire item or element, or for subsystems | Desenvolvimento de um item ou elemento com responsabilidades divididas entre cliente e fornecedor para o item ou elemento completo ou para os subsistemas |
| NOTE Customer and supplier are roles of the cooperating parties. | Clientes e fornecedor são papeis das partes colaboradoras |

|  |  |
| --- | --- |
| 1.28 diversity |  |
| different solutions satisfying the same requirement with the aim of **independence** (1.61) | Diferentes soluções que cumprem os mesmos requisitos com o proposito de independencia |
| EXAMPLE Diverse programming; diverse hardware. | Exemplo Diversas linguagens de programação, diversos hardwares |
| NOTE Diversity does not guarantee independence, but addresses certain types of **common cause failures** (1.14). | Duversity não garante independencia, mas resolve certos casos de common cause failures (1.14) |

|  |  |  |  |
| --- | --- | --- | --- |
| 1.29 dual-point failure | |  | |
| **failure** (1.39) resulting from the combination of two independent **faults** (1.42) that leads directly to the violation of a **safety goal** (1.108) | | **Falha resultante da combinação de duas falhas independentes que leva diretamente à violaçao de um safety goal** | |
| NOTE 1 Dual-point failures are multiple-point failures (1.76) of order 2.  Note 2 Dual-point failures that are addressed in ISO 26262 include those where one fault affects a safety-related element (1.113) and another fault affects the corresponding safety mechanism (1.111) intended to achieve or maintain a safe state (1.102).    NOTE 3 For a dual-point failure to directly violate a safety goal, the presence of both independent faults is necessary, i.e. the violation of a safety goal due to a combination of a residual fault (1.96) with a safe fault (1.101) is not considered a dual-point failure since the residual fault leads to a violation of a safety goal with or without the presence of a second independent fault. | | Note 1 Dual point failures são **multiple point failures** de ordem 2  Note 2 Dual-point failures que são resolvidos na ISO 26262 incluem aqueles onde uma falha afeta um **safety-related element** (1.113) e outra falha afeta o correspondente **safety mechanism** (1.111) que se pretende para alcançar ou manter um **safe state** (1.102).  Nota 3 para que um **dual-point failure** viole diretamente um safety goal, a presença de ambas as falhas independentes é necessaria, ie, a violação de um safety goal devido a uma combinação de um residual fault com uma safe fault não é considerada uma dual point failure desde que uma falha residual leva à violação de um safety goal com ou sem a presença de uma segunda falha independente | |
| 1.30 dual-point fault | |  | |
| individual **fault** (1.42) that, in combination with another independent fault, leads to a **dual-point failure** (1.29) | | Falha individual que em combinação com outra falha independente leva a uma dual point failure. | |
| NOTE 1 A dual-point fault can only be recognized after the identification of dual-point failure, e.g. from cut set analysis of a fault tree. | | Note 1 Uma dual point fault so pode ser reconhecida apos a identificação de uma dual point failure, eg, ? | |
| NOTE 2 See also **multiple-point fault** (1.77). | |  | |
| 1.31 electrical and/or electronic system | |  | |
| **E/E system** | |  | |
| **system** (1.129) that consists of electrical and/or electronic **elements** (1.32), including programmable electronic elements | |  | |
| EXAMPLE Power supply; sensor or other input device; communication path; actuator or other output device. | |  | |
| 1.32 element | |  | |
| **system** (1.129) or part of a system including **components** (1.15), hardware, software, **hardware parts** (1.55), and **software units** (1.125) | |  | |
| 1.33 embedded software | |  | |
| fully-integrated software to be executed on a processing **element** (1.32) | |  | |
| NOTE The processing element is normally a micro-controller, a field programmable gate array (FPGA) or an application-specific integrated circuit (ASIC), but it can also be a more complex **component** (1.15) or subsystem. | |  | |
| 1.34 emergency operation | |  | |
| degraded functionality from the state in which a **fault** (1.42) occurred until the transition to a **safe state** (1.102) is achieved as defined in the **warning and degradation concept** (1.140) | |  | |
| 1.35 emergency operation interval | |  | |
| specified time-span that **emergency operation** (1.34) is needed to support the **warning and degradation concept** (1.140) | |  | |
| NOTE Emergency operation is part of the **warning and degradation concept** (1.140). | |  | |
| 1.36 error | |  | |
| discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretically correct value or condition | |  | |
| NOTE 1 An error can arise as a result of unforeseen operating conditions or due to a **fault** (1.42) within the **system** (1.129), subsystem or **component** (1.15) being considered. | |  | |
| NOTE 2 | |  | |
| A fault can manifest itself as an error within the considered **element** (1.32) and the error can ultimately cause a **failure** (1.39). | |  | |
| 1.37 exposure | |  | |
| state of being in an **operational situation** (1.83) that can be **hazardous** (1.57) if coincident with the **failure mode** (1.40) under analysis | | Estado de estar numa situação operacional que poder ser perigosa se coincidente com o failure mode sob analise | |
|  | | | |
| E1 | E2 | E3 | E4 |
| Very Low Probability | Low Probability | Medium Probability | High Probability |
| Not Spec. | <0.01 | <0.1 | >0.1 |
| 1.38 external measure | |  | |
| measure that is separate and distinct from the **item** (1.69) which reduces or mitigates the **risks** (1.99) resulting from the item | |  | |

|  |  |
| --- | --- |
| 1.39 failure |  |
| termination of the ability of an **element** (1.32), to perform a function as required | Perda da habilidade de um elemento realizar uma função conforme requerido |
| NOTE Incorrect specification is a source of failure. | Nota Umaespecificação incorreta é fonte de uma failure |
| 1.40 failure mode |  |
| manner in which an **element** (1.32) or an **item** (1.69) fails | Modo no qual um element ou item falha |
| 1.41 failure rate |  |
| probability density of **failure** (1.39) divided by probability of survival for a hardware **element** (1.32) | Densidade de probabilidade de failure dividido pela probabilidade de sobrevivencia de um elemento de hardware |
| NOTE The failure rate is assumed to be constant and is generally denoted as Lambda. | A failure rate é considerada constante e denominada lambda |
| 1.42 fault |  |
| **ELEMENT – FAULT (Razão ou Condição) – FAILURE (Perda ou diminuição de funcionalidade)** | |
| abnormal condition that can cause an **element** (1.32) or an **item** (1.69) to fail | Condição anormal que pode provocar um elemento (1.32) ou item (1.69) to fail |
| NOTE 1 Permanent, intermittent and **transient faults** (1.134) (especially soft-errors) are considered. | Nota 1 Permanent, intermitent e transient faults (especialmente soft errors) são considerados |
| NOTE 2 An intermittent fault occurs time and time again, then disappears. This type of fault can occur when a **component** (1.15) is on the verge of breaking down or, for example, due to a glitch in a switch. Some **systematic faults** (1.131) (e.g. timing marginalities) could lead to intermittent faults. | Nota 2 Uma fault intermitente ocorre de tempos em tempos depois desaparece. Este tipo de fault pode acontecer quando um componente está à beira de deixar de funcionar, por exemplo devido a glitches numa switch. Algumas systematic faults (ex temporizações marginais) podem levar a faults intermitentes |

### 1.43 fault model

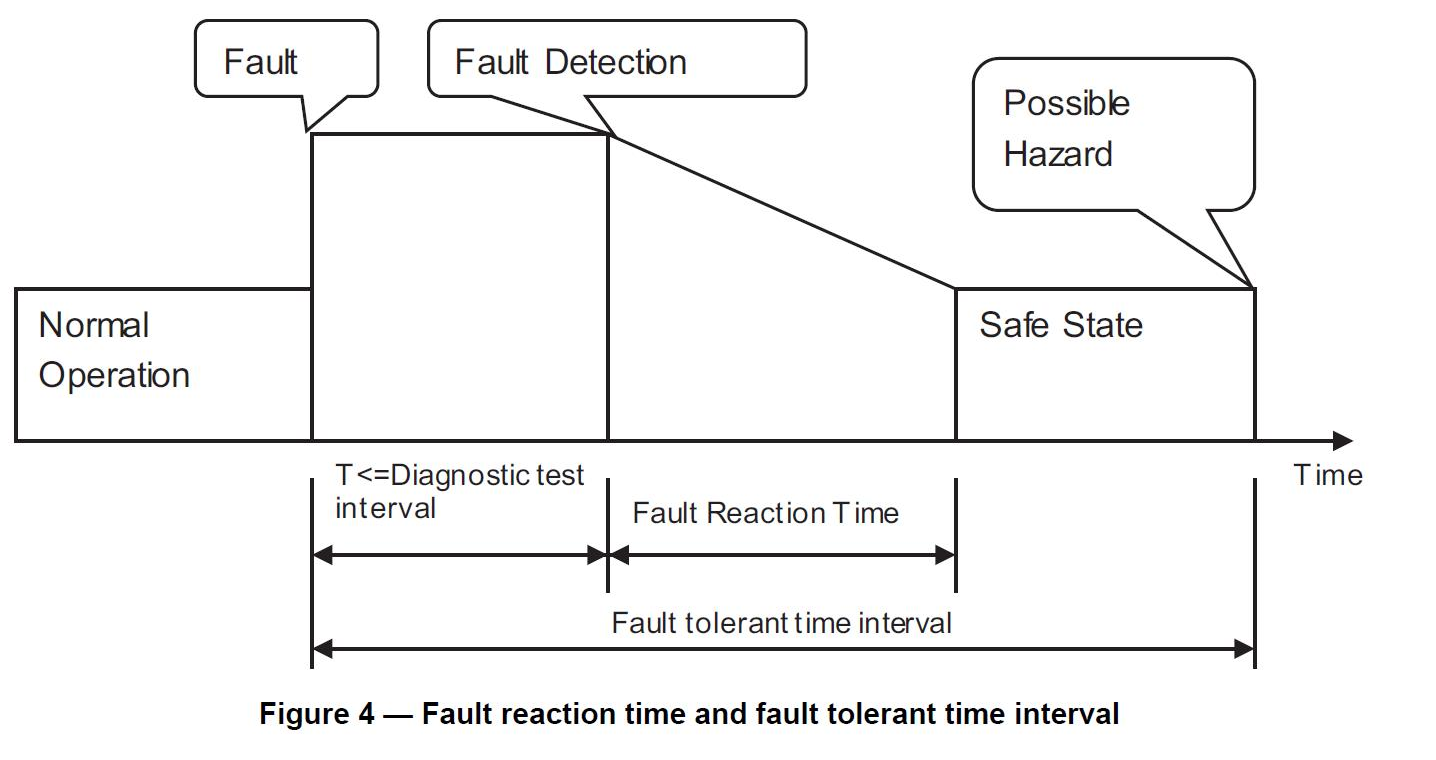
representation of **failure modes** (1.40) resulting from **faults** (1.42)

NOTE Fault models are generally based on field experience or reliability handbooks.

### 1.44 fault reaction time

time-span from the detection of a **fault** (1.42) to reaching the **safe state** (1.102)

See Figure 4.



### 1.45 fault tolerant time interval

time-span in which a **fault** (1.42) or faults can be present in a **system** (1.129) before a **hazardous** (1.57) event occurs

### 1.46 field data

data obtained from the use of an **item** (1.69) or **element** (1.32) including cumulative operating hours, all **failures** (1.39) and in-service anomalies

NOTE Field data normally comes from customer use.

### 1.47 formal notation

description technique that has both its syntax and semantics completely defined

EXAMPLE Z notation (Zed); NuSMV (symbolic model checker); Prototype Verification System (PVS); Vienna Development Method (VDM).

### 1.48 formal verification

method used to prove the correctness of a **system** (1.129) against the specification in **formal notation** (1.47) of its required behaviour

**1.49**

### freedom from interference

absence of **cascading failures** (1.13) between two or more **elements** (1.32) that could lead to the violation of a safety requirement

EXAMPLE 1 Element 1 is free of interference from element 2 if no **failure** (1.39) of element 2 can cause element 1 to fail.

EXAM

PLE 2 Element 3 interferes with element 4 if there exists a failure of element 3 that causes element 4 to fail.

### 1.50 functional concept

specification of the intended functions and their interactions necessary to achieve the desired behaviour

NOTE The functional concept is developed during the concept **phase** (1.89).

### 1.51 functional safety

absence of **unreasonable risk** (1.136) due to **hazards** (1.57) caused by **malfunctioning behaviour** (1.73) of **E/E systems** (1.31)

### 1.52 functional safety concept

specification of the **functional safety requirements** (1.53), with associated information, their **allocation** (1.1**)** to architectural **elements** (1.32), and their interaction necessary to achieve the **safety goals** (1.108)

|  |  |  |
| --- | --- | --- |
| 1.53 functional safety requirement | | Requisitos funcionais de segurança |
| specification of implementation-independent **safety** (1.103) behaviour, or implementation-independent **safety measure** (1.110), including its safety-related attributes | | Especificação de **safety** que é independente da implementação, ou Especificação de safety measure que é independente da implementação, incluindo os seus atributos safety related |
| NOTE 1 A functional safety requirement can be a safety requirement implemented by a safety-related **E/E system** (1.31), or by a safety-related **system** (1.129) of **other technologies** (1.84), in order to achieve or maintain a **safe state** (1.102) for the **item** (1.69) taking into account a determined **hazardous event** (1.59). | | NOTA Um functional safety requirement pode ser um safety requirement implementado por um safety related E/E ou por um safety related system ou por other technologies para que seja mantido um safe state para o item levando se em consideração um determinado hazardous event |
| Note 2 The functional safety requirements might be specified independently of the technology used in the concept **phase** (1.89), of product development. Safety-related attributes include information about **ASIL** (1.6). | | Nota 2 Os functional safety requirement podem ser especificados independentemente da tecnologia usada no concept phase do desenvolvimento do produto. Atributos safety related incluem informação sobre o ASIL. |
| 1.54 hardware architectural metrics | |  |
| metrics for the **assessment** (1.4) of the effectiveness of the hardware **architecture** (1.3) with respect to **safety** (1.103) | |  |
| NOTE The **single-point fault** (1.122) metric and the **latent fault** (1.71) metric are the hardware architectural metrics. | |  |
| 1.55 hardware part | |  |
| hardware which cannot be subdivided | |  |
| 1.56 harm |  | |
| physical injury or damage to the health of persons |  | |
| 1.57 hazard |  | |
| potential source of **harm** (1.56) caused by **malfunctioning behaviour** (1.73) of the **item** (1.69) |  | |
| NOTE This definition is restricted to the scope of ISO 26262; a more general definition is potential source of harm. |  | |
| 1.58 hazard analysis and risk assessment |  | |
| method to identify and categorize **hazardous events** (1.59) of **items** (1.69) and to specify **safety goals** (1.108) and **ASILs** (1.6) related to the prevention or mitigation of the associated hazards in order to avoid **unreasonable risk** (1.136) |  | |
| 1.59 hazardous event |  | |
| combination of a **hazard** (1.57) and an **operational situation** (1.83) |  | |

### 1.60 homogeneous redundancy

multiple but identical implementations of a requirement

### 1.61 independence

absence of **dependent failures** (1.22) between two or more **elements** (1.32) that could lead to the violation of a safety requirement, or organizational separation of the parties performing an action

NOTE By definition, **ASIL decomposition** (1.7) or **confirmation measures** (1.17) include requirements on independence.

### 1.62 independent failures

**failures** (1.39) whose probability of simultaneous or successive occurrence can be expressed as the simple product of their unconditional probabilities

### 1.63 informal notation

description technique that does not have its syntax completely defined

EXAMPLE Description in figure or diagram.

NOTE An incomplete syntax definition implies that the semantics are also not completely defined.

### 1.64 informal verification

**verification** (1.137) methods not considered as semi-formal or **formal verification** (1.48) techniques

EXAMPLE Design **review** (1.98); model review.

### 1.65 inheritance

passing attributes of requirements in an unchanged manner to the next level of detail during the development process

### 1.66 initial ASIL

**ASIL** (1.6) resulting from the hazard analysis or the ASIL resulting from a preceding **ASIL decomposition** (1.7)

NOTE The initial ASIL is the starting point for **ASIL decomposition** (1.7) or further ASIL decomposition.

### 1.67 inspection

examination of work products, following a formal procedure, in order to detect anomalies

NOTE 1 Inspection is a means of **verification** (1.137).

NOTE 2 Inspection differs from **testing** (1.134) in that it does not normally involve the operation of the associated **item** (1.69) or **element** (1.32).

NOTE 3 Any anomalies that are detected are usually addressed by rework, followed by re-inspection of the reworked products.

NOTE 4 A formal procedure normally includes a previously defined procedure, checklist, moderator and **review** (1.98) of the results.

### 1.68 intended functionality

behaviour specified for an **item** (1.69), **system** (1.129), or **element** (1.32) excluding **safety mechanisms** (1.111)

|  |  |
| --- | --- |
| 1.69 item |  |
| **system** (1.129) or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied | **System ou array de sistemas que implementam uma função (Implement a function in hardware and software) ao nivel do veiculo ao qual ISO 26262 aplica-se** |

### 1.70 item development

complete process of implementing an **item** (1.69)

### 1.71 latent fault

**multiple-point fault** (1.77) whose presence is not detected by a **safety mechanism** (1.111) nor perceived by the driver within the **multiple-point fault detection interval** (1.78)

### 1.72 lifecycle

entirety of **phases** (1.89) from concept through decommissioning of the **item** (1.69)

### 1.73 malfunctioning behaviour

**failure** (1.39) or unintended behaviour of an **item** (1.69) with respect to its design intent

### 1.74 model-based development

development that uses models to describe the functional behaviour of the **elements** (1.32) to be developed

NOTE Depending on the level of abstraction used for such a model, the model can be used for simulation or code generation or both.

### 11 1.75 modification

authorized alteration of an **item** (1.69)

NOTE 1 Modification is used in ISO 26262 with respect to re-use for **lifecycle** (1.72) tailoring.

NOTE 2

A change is applied during the lifecycle of an item, while a modification is applied to create a new item from an existing item.

### 1.76 multiple-point failure

**failure** (1.39), resulting from the combination of several independent **faults** (1.42), which leads directly to the violation of a **safety goal** (1.108)

NOTE For a multiple-point failure to directly violate a safety goal, the presence of all independent faults is necessary, i.e. the violation of a safety goal due to a combination of a **residual fault** (1.96) with other independent faults is not considered a multiple-point failure.

### 1.77 multiple-point fault

individual **fault** (1.42) that, in combination with other independent faults, leads to a **multiple-point failure** (1.76)

NOTE A multiple-point fault can only be recognized after the identification of multiple-point failure, e.g. from cut set analysis of a fault tree.

### 1.78 multiple-point fault detection interval

time span to **detect multiple-point fault** (1.77) before it can contribute to a **multiple-point failure** (1.76)

See Figure 4.

### 1.79 new development

process of creating an **item** (1.69) having previously unspecified functionality, a novel implementation of an existing functionality, or both

### 1.80 non-functional hazard

**hazard** (1.57) that arises due to factors other than incorrect functioning of the **E/E system** (1.31), safety-related **systems** (1.129) of **other technologies** (1.84), or **external measures** (1.38)

### 1.81 operating mode

perceivable functional state of an **item** (1.69) or **element** (1.32)

EXAMPLE **System** (1.129) off; system active; system passive; degraded operation; **emergency operation** (1.34).

### 1.82 operating time

cumulative time that an **item** (1.69) or **element** (1.32) is functioning

### 1.83 operational situation

scenario that can occur during a vehicle's life

EXAMPLE Driving; parking; maintenance.

### 1.84 other technology

technology different from E/E technologies within the scope of ISO 26262

EXAMPLE Mechanical technology; hydraulic technology.

NOTE Other technologies can either be considered in the specification of the **functional safety concept** (1.52) (see ISO 26262-3:2011, Clause 8 and Figure 2), during the **allocation** (1.1) of safety requirements (see ISO 26262-3 and ISO 26262-4), or as an **external measure** (1.38).

### 1.85 partitioning

separation of functions or **elements** (1.32) to achieve a design

NOTE Partitioning can be used for **fault** (1.42) containment to avoid **cascading failures** (1.13). To achieve **freedom from interference** (1.49) between partitioned design elements, additional non-functional requirements can be introduced.

### 1.86 passenger car

vehicle designed and constructed primarily for the carriage of persons and their luggage, their goods, or both, having not more than a seating capacity of eight, in addition to the driver, and without space for standing passengers

### 1.87 perceived fault

**fault** (1.42) whose presence is deduced by the driver within a prescribed time interval

EXAMPLE The fault can be directly perceived through obvious limitation of **system** (1.129) behaviour or performance.

### 1.88 permanent fault

**fault** (1.42) that occurs and stays until removed or repaired

NOTE Direct current (d.c.) faults, e.g. stuck-at and bridging faults, are permanent faults. **Systematic faults** (1.131) manifest themselves mainly as permanent faults.

### 1.89 phase

stage in the safety **lifecycle** (1.72) that is specified in a distinct part of ISO 26262

NOTE The phases in ISO 26262 are specified in distinct parts, i.e. ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7 specify, respectively, the phases of:

— con

cept,

— pro

duct development at the system level,

— pro

duct development at the hardware level,

— produ

ct development at the software level, and

— produ

ction and operation.

### 1.90 proven in use argument

evidence, based on analysis of **field data** (1.46) resulting from use of a **candidate** (1.12), that the probability of any **failure** (1.39) of this candidate that could impair a **safety goal** (1.108) of an **item** (1.69) that uses it meets the requirements for the applicable **ASIL** (1.6)

### 1.91 proven in use credit

substitution of a given set of **lifecycle** (1.72) **subphases** (1.128) with corresponding work products by a **proven in use argument** (1.90)

### 1.92 random hardware failure

**failure** (1.39) that can occur unpredictably during the lifetime of a hardware **element** (1.32) and that follows a probability distribution

NOTE Random hardware **failure rates** (1.41) can be predicted with reasonable accuracy.

### 1.93 reasonably foreseeable event

event that is technically possible and has a credible or measurable rate of occurrence

### 1.94 redundancy

existence of means in addition to the means that would be sufficient for an **element** (1.32) to perform a required function or to represent information

NOTE Redundancy is used in ISO 26262 with respect to achieving a **safety goal** (1.108) or a specified safety requirement, or to representing safety-related information.

EXAMPLE 1 Duplicated functional **components** (1.15) can be an instance of redundancy for the purpose of increasing **availability** (1.8) or allowing **fault** (1.42) detection.

EXAMPLE 2 The addition of parity bits to data representing safety-related information provides redundancy for the purpose of allowing fault detection.

### 1.95 regression strategy

strategy to verify that an implemented change did not affect the unchanged, existing and previously verified parts or properties of an **item** (1.69) or an **element** (1.32)

### 1.96 residual fault

portion of a **fault** (1.42) that by itself leads to the violation of a **safety goal** (1.108), occurring in a hardware **element** (1.32), where that portion of the fault is not covered by **safety mechanisms** (1.111)

NOTE This presumes that the hardware element has safety mechanism coverage for only a portion of its faults.

EXAM

PLE If low (60 %) coverage is claimed for a **failure mode** (1.40), the other 40 % of that same failure mode is the residual fault.

### 1.97 residual risk

**risk** (1.99) remaining after the deployment of **safety measures** (1.110)

### 1.98 review

examination of a work product, for achievement of the intended work product goal, according to the purpose of the review

NOTE Reviews can be supported by checklists.

|  |  |
| --- | --- |
| 1.99 risk |  |
| combination of the probability of occurrence of **harm** (1.56) and the **severity** (1.120) of that harm | Combinação da probabilidade da ocorrência de um harm e a severity (S0, S1, S2, S3) daquele harm |

### 1.100 robust design

design that has the ability to function correctly in the presence of invalid inputs or stressful environmental conditions

NOTE Robustness can be understood as follows:

— for software, robustness is the ability to respond to abnormal inputs and conditions;

— for hardware, robustness is the ability to be immune to environmental stress and stable over the service life within design limits;

— in the context of ISO 26262, robustness is the ability to provide safe behaviour at boundaries.

### 1.101 safe fault

**fault** (1.42) whose occurrence will not significantly increase the probability of violation of a **safety goal** (1.108)

NOTE 1 As shown in ISO 26262-5:2011, Annex B, both non-safety and **safety-related elements** (1.113) can have safe faults.

NOTE 2 **Single-point faults** (1.122), **residual faults** (1.96) and dual-point faults do not constitute safe faults.

NOTE 3 Unless shown relevant in the safety concept, **multiple-point faults** (1.77) with higher order than 2 can be considered as safe faults.

### 1.102 safe state

**operating mode** (1.81) of an **item** (1.69) without an unreasonable level of **risk** (1.99)

EXAMPLE Intended operating mode; degraded operating mode; switched-off mode.

### 1.103 safety

absence of **unreasonable risk** (1.136)

### 1.104 safety activity

activity performed in one or more **subphases** (1.128) of the safety **lifecycle** (1.72)

### 1.105 safety architecture

set of **elements** (1.32) and their interaction to fulfil the safety requirements

### 1.106 safety case

argument that the safety requirements for an **item** (1.69) are complete and satisfied by evidence compiled from work products of the safety activities during development

NOTE Safety case can be extended to cover **safety** (1.103) issues beyond the scope of ISO 26262.

### 1.107 safety culture

policy and strategy used within an organization to support the development, production and operation of safety-related systems (1.129)

NOTE See ISO 26262-2:2011, Annex B.

|  |  |
| --- | --- |
| 1.108 safety goal |  |
| top-level safety requirement as a result of the **hazard analysis and risk assessment** (1.58) | Requisito de segurança de alto nivel como resultado da **hazard analysis and risk assessment** (1.58) |
| NOTE One safety goal can be related to several **hazards** (1.57), and several safety goals can be related to a single hazard. |  |

### 

|  |  |
| --- | --- |
| 1.109 safety manager | VER COM O PRADO |
| role filled by the person responsible for the **functional safety** (1.51) management during the **item** (1.69) development | Papel preenchido pela pessoa responsável pela gestão do functional safety durante a fase de desenvolvimento do item |

### 1.110 safety measure

activity or technical solution to avoid or control **systematic failures** (1.130) and to detect **random hardware failures** (1.92) or control random hardware failures, or mitigate their harmful effects

NOTE 1 Examples of safety measures are FMEA and software without the use of global variables.

NOTE 2 Safety measures include **safety mechanisms** (1.111).

### 1.111 safety mechanism

technical solution implemented by E/E functions or **elements** (1.32), or by **other technologies** (1.84), to detect **faults** (1.42) or control **failures** (1.39) in order to achieve or maintain a **safe state** (1.102)

NOTE 1 Safety mechanisms are implemented within the **item** (1.69) to prevent faults from leading to **single-point failures** (1.121) or to reduce residual failures and to prevent faults from being latent. e safety mechanism is either ble to transition to, or maintain, the item in a safe state, or b) able to alert the driver such that the driver is expected to control the effect of the **failure** (1.39),

as defined in the **functional safety concept** (1.52).

### 1.112 safety plan

plan to manage and guide the execution of the **safety activities** (1.104) of a project including dates, milestones, tasks, deliverables, responsibilities and resources

### 1.113 safety-related element

**element** (1.32) that has the potential to contribute to the violation of or achievement of a **safety goal** (1.108)

NOTE Fail-safe elements are considered safety-related if they can contribute to at least one safety goal.

### 1.114 safety-related function

function that has the potential to contribute to the violation of a **safety goal** (1.108)

### 1.115 safety-related special characteristic

characteristic of an **item** (1.69) or an **element** (1.32), or else their production process, for which reasonably foreseeable deviation could impact, contribute to, or cause any potential reduction of **functional safety** (1.51)

NOTE 1 Term special characteristics are defined in ISO/TS 16949.

NOTE

2 Safety-related special characteristics are derived during the development **phase** (1.89) of the item or the elements.

EXAMPLE Temperature range; expiration date; fastening torque; production tolerance; configuration.

### 1.116 safety validation

assurance, based on examination and tests, that the **safety goals** (1.108) are sufficient and have been achieved

NOTE ISO 26262-4 provides suitable methods for validation.

### 1.117 semi-formal notation

description technique whose syntax is completely defined but whose semantics definition can be incomplete

EXAMPLE System Analysis and Design Techniques (SADT); Unified Modeling Language (UML).

### 1.118 semi-formal verification

**verification** (1.137) that is based on a description given in **semi-formal notation** (1.117)

EXAMPLE Use of test vectors generated from a semi-formal model to test that the **system** (1.129) behaviour matches the model.

### 1.119 service note

documentation of **safety** (1.103) information to be considered when performing maintenance procedures for the **item** (1.69)

EXAMPLE **Safety-related special characteristic** (1.115); safety operation that can be required.

|  |  |  |  |
| --- | --- | --- | --- |
| 1.120 severity | |  | |
| estimate of the extent of **harm** (1.56) to one or more individuals that can occur in a potentially **hazardous** (1.57) situation | | Estimativa da extensão do harm(1.56) para uma ou mais pessoas que pode acontecer numa situação potencialmente perigosa | |
| NOTE The parameter “S” in **hazard analysis and risk assessment** (1.58) represents the potential severity of harm. | | Nota O Parâmetro S em hazard analysis and risk assessment(1.58) representa a severidade potencial de harm | |
| S0 | S1 | S2 | S3 |
| No Injuries | Light & Moderate Injuries | Severe and Life  threatening Injuries | Life  threatening Injuries,  Fatal Injuries |
| AIS 0 | AIS 1 & 2 | AIS 3 & 4 | AIS 5 & 6 |

### 1.121 single-point failure

**failure** (1.39) that results from a **single-point fault** (1.122) and that leads directly to the violation of a **safety goal** (1.108)

NOTE 1 A single-point failure is equivalent to a residual failure for an **element** (1.32) with 0 % **diagnostic coverage** (1.25).

NOTE 2 If at least one **safety mechanism** (1.111) is defined for an HW element (e.g. a watchdog for a microcontroller), then no **faults** (1.42) of the considered hardware element are single-point faults.

### 1.122 single-point fault

**fault** (1.42) in an **element** (1.32) that is not covered by a **safety mechanism** (1.111) and that leads directly to the violation of a **safety goal** (1.108)

NOTE See also **single-point failure** (1.121).

### 1.123 software component

one or more **software units** (1.125)

### 1.124 **software tool**

computer program used in the development of an **item** (1.69) or **element** (1.32)

### 1.125 **software unit**

atomic level **software component** (1.123) of the software **architecture** (1.3) that can be subjected to stand-alone **testing** (1.134)

**17**

### 1.126 **special-purpose vehicle**

vehicle intended to perform a function that requires special body arrangements, equipment or both

EXAMPLE Motor caravan; armoured vehicle; ambulance; hearse; trailer caravan; mobile crane.

NOTE

ECE TRANS/WP.29/78/Rev.1/Amend.2 provides definitions for special-purpose vehicles.

### 1.127 statement coverage

percentage of statements within the software that have been executed

### 1.128 subphase

subdivision of a stage in the safety **lifecycle** (1.72) that is specified in a distinct clause of ISO 26262

EXAMPLE **Hazard analysis and risk assessment** (1.58) is a subphase of the safety lifecycle specified in ISO 26262-3:2011, Clause 7.

|  |  |
| --- | --- |
| 1.129 system |  |
| set of **elements** (1.32) that relates at least a sensor, a controller and an actuator with one another | Conjunto de **elements** que relaciona um sensor, um controlador e um atuador |
| NOTE 1 The related sensor or actuator can be included in the system, or can be external to the system. | Nota 1 O sensor ou atuador pode ser incluido no sistema ou pode ser exterior ao sistema |
| NOTE 2 An element of a system can also be another system. | Nota 2 Um elemento de um sistema pode ser outro sistema |
|  | |

### 1.130 systematic failure FAILURE (Perda ou diminuição de funcionalidade) é o resultado de uma fault. FAILURE é a manifestação de um FAULT

**failure** (1.39), related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

### 1.131 systematic fault FAULT é a RAZÃO DE UMA FAILURE

**fault** (1.42) whose **failure** (1.39) is manifested in a deterministic way that can only be prevented by applying process or design measures

### 1.132 technical safety concept

specification of the **technical safety requirements** (1.133) and their **allocation** (1.1) to **system** (1.129) **elements** (1.32) for implementation by the system design

### 1.133 technical safety requirement

requirement derived for implementation of associated **functional safety requirements** (1.53)

NOTE The derived requirement includes requirements for mitigation.

### 1.134 testing

process of planning, preparing, and operating or exercising an **item** (1.69) or an **element** (1.32) to verify that it satisfies specified requirements, to detect **anomalies** (1.2), and to create confidence in its behaviour

### 1.135 transient fault

**fault** (1.42) that occurs once and subsequently disappears

NOTE Transient faults can appear due to electromagnetic interference, which can lead to bit-flips. Soft errors such as Single Event Upset (SEU) and Single Event Transient (SET) are transient faults.

### 1.136 unreasonable risk

**risk** (1.99) judged to be unacceptable in a certain context according to valid societal moral concepts

### 1.137 verification

determination of completeness and correct specification or implementation of requirements from a **phase** (1.89) or **subphase** (1.128)

### 1.138 verification review

**verification** (1.137) activity to ensure that the result of a development activity fulfils the project requirements, or technical requirements, or both

NOTE 1 Individual requirements on verification reviews are given in specific clauses of individual parts of ISO 26262.

NOTE

2 The goal of verification reviews is technical correctness and completeness of the **item** (1.69) or **element** (1.32) with respect to use cases and **failure modes** (1.40).

EXAMPLE

Technical **review** (1.98); **walk-through** (1.139); **inspection** (1.67).

### 1.139 walk-through

systematic examination of **work products** (1.142) in order to detect anomalies

NOTE 1 Walk-through is a means of **verification** (1.137).

NOTE

2 Walk-through differs from **testing** (1.134) in that it does not normally involve the operation of the associated **item** (1.69) or **element** (1.32).

NOTE 3 A

ny anomalies that are detected are usually addressed by rework, followed by a walk-through of the reworked work products.

EXAM

PLE During a walk-through, the developer explains the work product step-by-step to one or more assessors. The objective is to create a common understanding of the work product and to identify any anomalies within the work product. Both **inspections** (1.67) and walk-throughs are types of peer **review** (1.98), where a walk-through is a less stringent form of peer review than an inspection.

### 1.140 warning and degradation concept

specification of how to alert the driver of potentially reduced functionality and of how to provide this reduced functionality to reach a **safe state** (1.102)

### 1.141 well-trusted

previously used without known **safety** (1.103) **anomalies** (1.2)

EXAMPLE Well-trusted design principle; well-trusted tool; well-trusted hardware **component** (1.15).

### 1.142 work product

result of one or more associated requirements of ISO 26262

NOTE A reference can be an independent document containing the complete information of a work product or a list of references to the complete information of a work product.

AIS Abbreviated Injury Scale

ASIC Application-Specific Integrated Circuit

ASIL Automotive Safety Integrity Level (see definition 1.6)

BIST Built-In Self-Test

CAN Controller Area Network

CCF Common Cause Failure (see definition 1.14)

COTS Commercial Off The Shelf

CPU Central Processing Unit

CRC Cyclic Redundancy Check

DC Diagnostic Coverage (see definition 1.25)

d.c. Direct Current

DIA Development Interface Agreement (see definition 1.24)

DSC Dynamic Stability Control

ECU Electronic Control Unit

EDC Error Detection and Correction

E/E system Electrical and/or Electronic system (see definition 1.31)

EMC Electromagnetic Compatibility

EMI Electromagnetic Interference

ESD Electrostatic Discharge

ESC Electronic Stability Control

ETA Event Tree Analysis

FPGA Field Programmable Gate Array

FIT Failures In Time

FMEA Failure Mode and Effects Analysis

FTA Fault Tree Analysis

HAZOP HAZard and Operability analysis

HSI Hardware-Software Interface

HW Hardware

H&R Hazard analysis and Risk assessment (see definition 1.58)

IC Integrated Circuit

I/O Input – Output

MC/DC Modified Condition/Decision Coverage

MMU Memory Management Unit

MPU Memory Protection Unit

Licensed to Critical Software SA / Mr. Castanheira ISO Store order #: 10-1360272/Downloaded: 2013-11-05 Single user licence only, copying and networking prohibited **ISO 26262-1:2011(E) 20** © ISO 2011 – All rights reserved

MUX MUltipleXer

OS Operating System

PLD Programmable Logic Device

PMHF Probabilistic Metric for random Hardware Failures

QM Quality Management

RAM Random Access Memory

ROM Read Only Memory

RFQ Request For Quotation

SIL Safety Integrity Level

SOP Start Of Production

SRS System Requirements Specification

SW Software

UML Unified Modeling Language

V&V Verification and Validation

XML eXtensible Markup Language