Chapter 2
Why Functional Safety in Road Vehicles?

It took a while until functional safety started to play a significant role in the automotive industry in comparison to other industries. Customers, producers and dealers networks demanded more functionality and complexity of the products and market. One of the major reasons was that mechanical engineers primarily dominated the entire automobile engineering industry. The same industry developed the safety mechanism in the related field, without relying on electronics or even software. Therefore, these safety mechanisms were first and foremost based on a robust design as well as hydraulic or pneumatic safety mechanisms. With the increased amount of automation and electrification of essential vehicle functions and the desire to make these systems applicable for higher speeds and dynamics, electrification was the only way to go. Also the earlier concepts steer-by-wire and brake-by-wire, right up until today's autonomous or highly automated driving systems, make the usage of software based safety mechanisms unavoidable. If you look at one of today's common mid-range cars such as the 'Volkswagen Golf', you will find about 40 control units, which are still mainly networked by a CAN-Bus. It is "State-of-Science and Technology" that no complex vehicle systems could be realized without a systems approach. One of the main challenges of ISO 26262 [1] was that various methods, methodology, principles, best practices had been established but there was no consistent system development approach.

The main task in the development of ISO 26262 was to agree upon one basic understanding of system engineering. Therefore, it is not a surprise that the word 'system engineering' appears quite often in the introduction.

2.1 Risk, Safety and Functional Safety in Automobiles

In general, risk is described as a possible event with a negative impact. The Greek origin of the word risk had been also used for hazard or danger. In regards to product safety it is referred to as the cross product of probability of occurrence and

H.-L. Ross, *Functional Safety for Road Vehicles*,
DOI 10.1007/978-3-319-33361-8_2

hazard/danger. There are different opinions on the term and definition of risk in the economic literature. Definitions vary from 'danger of a variance of error' to the mathematical definition 'risk = probability × severity'.

The general definition is as follows: The probability of damage or loss as consequence of a distinct behavior or events; this refers to hazardous/dangerous situations in which unfavorable consequences may occur but do not necessarily have to.

On the one hand, risk can be traced back etymologically to 'riza' (Greek = root, basis); see also 'risc' (Arabic = destiny). On the other hand, risk can be referred to 'ris(i)co' (Italian); "The cliff, which has to be circumnavigated". 'Safety' derives from Latin and could be translated as 'free from worry' (se cura = without worry). Today, the topic of safety is viewed in various different contexts for example, in regards to economic safety, environmental safety, admittance and access security but also in terms of work safety, plant and machinery safety and vehicle safety. The term safety varies significantly from just only functional safety.

In relation to technical systems or products, safety is described as the freedom of unacceptable risks. 'Damage' is generally seen as harm or impairment of people as well as the environment.

There are various distinctions of hazard:

- Chemical reactions of substances, materials etc. lead to fire, explosions, injuries, health impairments, poisoning, environmental damage etc.
- Toxic substances lead to poisoning (also carbon monoxide), injuries (consequence of for example degassing of batteries, error reactions of the driver or mistakes of the auto repair shop staff), other damages etc.
- High currents and especially high voltages lead to damages (in particular personal protection).
- Radiations (nuclear, but also radiations like alpha particle semiconductor).
- Thermic (damages due to overheating, singe, fire, smoke etc.).
- Kinetics (deformation, movement, accelerated mass can lead to injuries).

The potential reasons for hazard cannot be easily defined, since chemical reactions can also lead to poisoning and overheating, to fire and thus also to smoke intoxication. Similar correlations appear in high currents or excessive voltages. High voltages lead to burns when touching but can also cause fires. Overvoltage is often seen as a non-functional risk or hazard. This is why most of the standards encounter such hazards with design constraints. A contact safety device or touch guard on a safety plug connector is a typical example. This leads us to the following point of view and distinction of functional safety.

Functional safety is generally described as the correct technical reaction of a technical system in a defined environment, with a given defined stimulation as an input of the technical system. ISO 26262 defines functional safety as absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems. Also, the error or failure reactions of mechanic or hydraulic safety components are

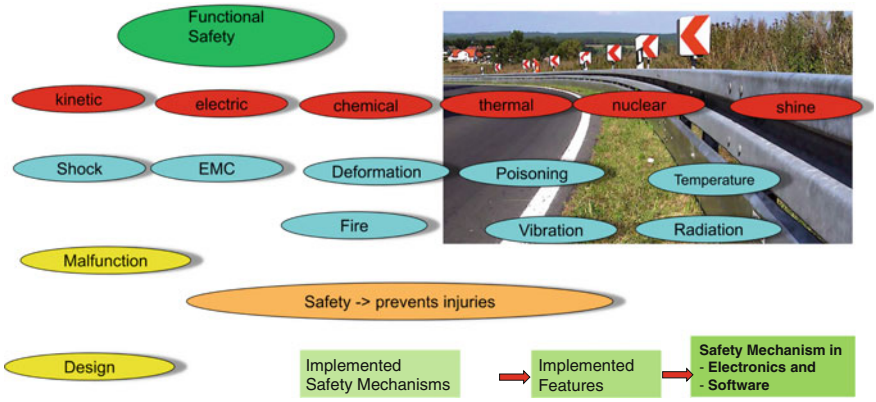

Fig. 2.1 Functional safety—safety design, control of forces and energies

controlled by electronic safety mechanisms in mechatronic systems. This distinction will be discussed later in reference to ISO 26262 (Fig. 2.1).

Functional safeguarding with hydraulic systems has always been used for automobiles. A typical example would be the dual-circuit braking system or the hydraulic steering system. Electronic and software based functional safety mechanisms were introduced as for example the ABS (Anti-Wheel-Blocking-System) for brake systems 30 years ago. Prior to that the necessary safety was only established by sufficient robust system and safe component characteristics (meaning through design).

The following definitions of risk, hazard/danger and integrity have been added to *DIN EN 61508-1:2002–11:*

Citation from IEC 61508 [2], *Part 5, A5:*
A.5 Risk and Safety Integrity

It is important that the distinction between risk and safety integrity be fully appreciated. Risk is a measure of the probability and consequence of a specified hazardous event occurring. This can be evaluated for different situations [EUC risk, risk required to meet the tolerable risk, actual risk (see Fig. A.1)]. The tolerable risk is determined on a societal basis and involves consideration of societal and political factors. Safety integrity applies solely to the E/E/PE safety-related systems, other technology safety related-systems and external risk reduction facilities and is a measure of the likelihood of those systems/facilities satisfactorily achieving the necessary risk reduction in respect of the specified safety functions. Once the tolerable risk has been set, and the necessary risk reduction estimated, the safety integrity requirements for the safety-related systems can be allocated. (see 7.4, 7.5 and 7.6 of IEC 61508-1) (Fig. 2.2).

Furthermore, IEC 61508 shows the following figure to explain coherences (Fig. 2.3):

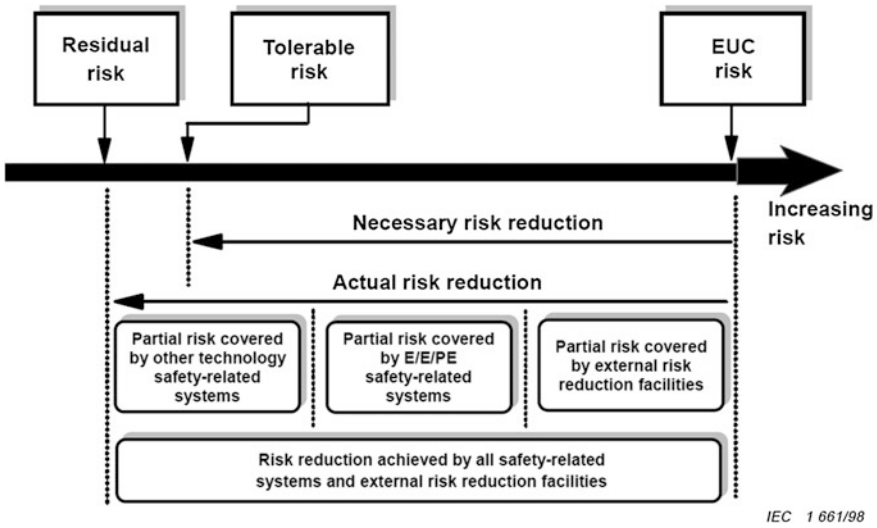

Fig. 2.2 Risk reduction according to IEC 61508 (*Source* IEC 61508-1:2011)

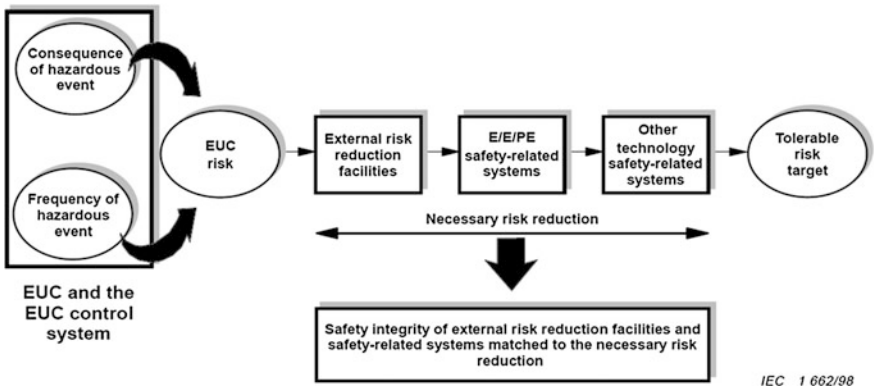

Fig. 2.3 Risk- and safety integrity according to IED 61508 (*Source* IEC 61508-1:2011)

ISO 26262 defines the relation of risk, danger and safety integrity differently. The term safety integrity is not directly used in ISO 26262. In particular the term EUC (Equipment under Control) is not used at all. EUC could be explained as "device or system, which should be controlled by means of functional safety measures". Under certain limiting conditions ISO 26262 admits to develop a desired vehicle function that is safety-related on its own. In this case, the system does not receive safety through EUC itself. Technically, according to IEC 61508, EUC and the safety functions have to cause an error at the same time in order to create a hazardous situation. If for example a hydraulic braking system was the

EUC, which in its function can be monitored by an EE-system, errors of the hydraulic systems could be avoided by the EE-system. The automobile industry relies here on other technology and engineering of the electronic safety system will be considered as a fail-safe-system.

As mentioned previously, ISO 26262 defines functional safety as freedom of unacceptable risks based on hazards, which are caused by malfunctional behavior of E/E-systems. However, interactions of systems with E/E-functions are included as well and therefore also mechatronic systems. Whether pure mechanical systems really show not any interactions with E/E is doubtful. Furthermore, the introduction chapter of ISO 26262, which describes the scope of the norm, excludes hazards such as electric shock, fire, smoke, heat, radiation, poisoning, inflammation, (chemical) reactions, corrosion, release of energy or comparable hazards, as long as the failure was not caused by electrical components. Such hazards are caused more by the battery as well as the poisonous electrolytes in the capacitors. Whether a motor winding is an electrical device or a mechanical component is also questionable.

In general, it will be difficult to assign the ASIL with non-functional hazards. Such components have so far been construed sturdily in order to avoid any danger. In the context of the hazard and risk analysis it is difficult to allocate a specific ASIL to a weakness in design or construction.

ISO 26262 also excludes functional performances. Therefore, safety-in-use or functional inadequacy means functions, which already lead to a hazard, even if they functioning correctly are generally excluded in advance.

All explain the correlation of risk and damage as follows:

ISO 26262, part 3, appendix B1:

For this analytical approach a risk (R) can be described as a function (F), with the frequency of occurrence (f) of a hazardous event, the ability of the avoidance of specific harm or damage through timely reactions of the persons involved (controllability: C), and the potential severity (S) of the resulting harm or damage:

$$R = F(f, C, S)$$

The frequency of occurrence f is, in turn, influenced by several factors. One factor to consider is how frequently and for how long individuals find themselves in a situation where the aforementioned hazardous event can occur. In ISO 26262 this is simplified to be a measure of the probability of the driving scenario taking place in which the hazardous event can occur (Exposure: E). Another factor is the failure rate of the item that could lead to the hazardous event (Failure rate: λ). The failure rate is characterized by

hazardous hardware random failures and systematic faults that remained in the system:

$$f = E \times C$$

Hazard analysis and risk assessment is concerned with setting requirements for the item such that unreasonable risk is avoided.

ISO 26262 mentions normative methods that describe a systematic derivation of the potential risk, which may originate from the investigated of the considered Item (vehicle system), based on a hazard analysis and risk assessment. Hazard or risk analyses are not normatively defined in other safety standards. Either the requirements for these methods are listed or the method itself is exemplarily described (Fig. 2.4).

The reduction of risk cannot be achieved with the activities and methods mentioned in ISO 26262 if a function is not suitable, inadequate suitable, inadequate or falsely indicated for certain safety related functions. This represents a special challenge, considering that ISO 26262 does not directly addresses a EUC (Equipment under Control, e.g. a system, machinery or vehicle, which should be controlled safety-related systems) or the distinction between safety functions of designated safety requirements for on-demand (low demand) or continuous mode (high demand) safety systems. How is it possible to find out whether or not reactions of a vehicle system or certain measurements are sufficient, tolerable or safety-related appropriate?

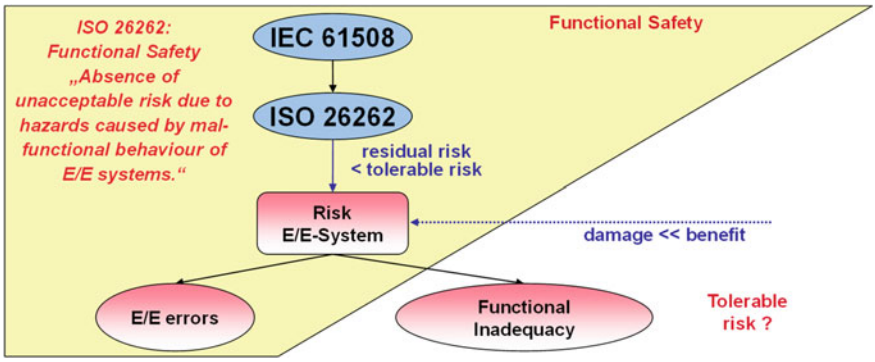

Fig. 2.4 Distinction of hazards, based on correctly functioning systems (*Reference* unpublished research project [7])

2.2 Quality Management System

Prof. Dr. rer. nat. Dr. oec. h. c. Dr.-Ing. E. h. Walter Masing, is also called the father of quality management systems, at least in Germany. His standard reference "Masing Handbook Quality Management" had a substantial influence on the standardization and interpretation of quality management systems.

A lot of methods and principles of management systems are explained already in ISO 9000. However, in 2005, statistics and trial methods became less relevant as the process approach became more and more important.

In the automotive industry an addition to ISO 9001 exists, called ISO TS 16949 [3]. It describes additions especially to the product development and production, which developed into standards in this industry. Today, in order for a distributor to be able to supply automotive manufacturers, the certification of ISO TS 16949 is an essential basic. Manufacturers from Asia still refer to different standards, based on historical reasons. Especially in Japan, quality requirements focus more on the ideals of the six-sigma-philosophy (for example DFSS, Design for Six Sigma). In particular the static analysis and trial methods mentioned in Masing's book, in DSFF as well as in functional safety are often based on comparable principles. ISO TS 16949 asks in the following chapters for essential basics for functional safety according to ISO 26262:

ISO TS 16949, 4.2.3.1: Engineering specifications

The organization shall have a process to assure the timely review, distribution and implementation of all customer engineering standards/specifications and changes based on customer-required schedule. Timely review should be as soon as possible, and shall not exceed two working weeks.

The organization shall maintain a record of the date on which each change is implemented in production. Implementation shall include updated documents.

NOTE A change in these standards/specifications requires an updated record of customer production part approval when these specifications are referenced on the design record or if they affect documents of production part approval process, such as control plan, FMEAs, etc.

Here, the norm refers to document and change management, application of necessary norms and standards, methods, output/work results and the regulation of responsibility (clearance), which is mentioned in ISO 26262 as QM-methods.

ISO TS 16949, 5.6.1.1 Quality management system performance

These reviews shall include all requirements of the quality management system and its performance trends as an essential part of the continual improvement process.

Part of the management review shall be the monitoring of quality objectives, and the regular reporting and evaluation of the cost of poor quality (see 8.4.1 and 8.5.1).

These results shall be recorded to provide, as a minimum, evidence of the achievement of

- *the quality objectives specified in the business plan, and*
- *customer satisfaction with product supplied.*

This explains the fact that product development as well as the satisfaction of the products delivered has to be documented and proven. If it concerns safety related features this may affect the customer substantially.

ISO TS 16949, 5.6.2: Review input
ISO 9001:2000, Quality management systems—Requirements

5.6.2 Review input
The input to management review shall include information on

a) results of audits,
b) customer feedback,
c) process performance and product conformity,
d) status of preventive and corrective actions,
e) follow-up actions from previous management reviews,
f) changes that could affect the quality management system, and
g) recommendations for improvement.

This list can also be seen as a "safety culture" in infrastructure requirements and essential for functional safety.

ISO TS 16949, 5.6.2.1: Review input

Input to management review shall include an analysis of actual and potential field-failures and their impact on quality, safety or the environment.

This chapter refers directly to the essential field observations, which are also required by the government in the context of product liability laws. It also directly refers to safety defects.

ISO TS 16949, 5.6.3: Review output
ISO 9001:2000, Quality management systems—Requirements

5.6.3 Review output
The output from the management review shall include any decisions and actions related to

a) improvement of the effectiveness of the quality management system and its processes,
b) improvement of product related to customer requirements, and
c) resource needs.

There are further additions mentioned to this topic in particular in ISO 26262.

ISO TS 16949, 6: Resource management

6.1 Provision of resources

ISO 9001:2000, Quality management systems—Requirements 6 Resource management 6.1 Provision of resources The organization shall determine and provide the resources needed (a) to implement and maintain the quality management system and continually improve its effectiveness, and (b) to enhance customer satisfaction by meeting customer requirements.

6.2 Human resources

6.2.1 General

ISO 9001:2000, Quality management systems—Requirements 6.2 Human resources 6.2.1 General

Personnel performing work affecting product quality shall be competent on the basis of appropriate education, training, skills and experience.

Sections 6.1 and 6.2 show, that also in the development stage essential requirements of people, their qualifications and the organization of product creation are well defined according to quality management systems.

ISO TS 16949, 7.3.1.1: Multidisciplinary approach

The organization shall use a multidisciplinary approach to prepare for product realization, including

- *development/finalization and monitoring of special characteristics,*
- *development and review of FMEAs, including actions to reduce potential risks, and*
- *development and review of control plans.*

NOTE A multidisciplinary approach typically includes the organization's design, manufacturing, engineering, quality, production and other appropriate personnel.

This cross-functional approach of ISO TS 16949 defines the basis for a necessary safety culture as the foundation of functional safety and address directly FMEAs as a mayor quality analysis method.

ISO TS 16949, 7.3.2.3: Special characteristics

The organization shall identify special characteristics [see 7.3.3 d] and

- *include all special characteristics in the control plan,*
- *comply with customer-specified definitions and symbols, and*
- *identify process control documents including drawings, FMEAs, control plans, and operator instructions with the customer's special characteristic symbol or the organization's equivalent symbol or notation to include those process steps that affect special characteristics.*

NOTE Special characteristics can include product characteristics and process parameters.

This chapter defines the way safety requirements were handled previously in the automobile industry. In particular "special characteristics" are still used for a safety-related design parameter of mechanic parts. The paragraph also defines the basics for the production of safety related components.

ISO TS 16949, 7.3.3.1: Product design output—Supplemental

The product design output shall be expressed in terms that can be verified and validated against product design input requirements. The product design output shall include

- *Design FMEA, reliability results,*
- *product special characteristics and specifications,*
- *product error-proofing, as appropriate,*
- *product definition including drawings or mathematically based data,*
- *product design reviews results, and*
- *diagnostic guidelines where applicable.*

This is a list of the output of product development, which had to be extended in ISO 26262 for the relevant safety related work-products and components. This output would for example be part of the safety case in a safety related product development.

ISO TS 16949, 7.3.3.2: Manufacturing process design output

The manufacturing process design output shall be expressed in terms that can be verified against manufacturing process design input requirements and validated. The manufacturing process design output shall include

- *specifications and drawings,*
- *manufacturing process flow chart/layout,*
- *manufacturing process FMEAs,*
- *control plan (see 7.5.1.1),*
- *work instructions,*
- *process approval acceptance criteria,*
- *data for quality, reliability, maintainability and measurability,*
- *results of error-proofing activities, as appropriate, and*
- *methods of rapid detection and feedback of product/manufacturing process nonconformities.*

This list adds to the necessary output/work-products during production. ISO 26262 rarely mentions any further requirements since this area is well regulated by quality management systems.

ISO TS 16949, 7.5.1.1: Control plan

The organization shall

- *develop control plans (see annex A) at the system, subsystem, component and/or material level for the product supplied, including those for processes producing bulk materials as well as parts, and*
- *have a control plan for pre-launch and production that takes into account the design FMEA and manufacturing process FMEA outputs. The control plan shall*
- *list the controls used for the manufacturing process control,*
- *include methods for monitoring of control exercised over special characteristics (see 7.3.2.3) defined by both the customer and the organization,*
- *include the customer-required information, if any, and*
- *initiate the specified reaction plan (see 8.2.3.1) when the process becomes unstable or not statistically capable. Control plans shall be reviewed and updated when any change occurs affecting product, manufacturing process, measurement, logistics, supply sources or FMEA (see 7.1.4).*

NOTE Customer approval may be required after review or update of the control plan.

ISO TS16949 describes the requirements of production control regarding the precedent development and required analyses, for example FMEAs, in detail. Analyses for product development are required—even if these products can be developed according to quality management systems but without any safety requirements.

2.2.1 Quality Management Systems from the Viewpoint of ISO 26262

Quality management is not mentioned very consistent in ISO 26262. The requirements set are the fundamentals, which enable any functional safety method to be applied in the automotive industry. Content wise, the appendix of part 2 ISO 26262 raises many interesting topics covering safety culture. ISO 26262 shortly summarizes the fundamental requirements as follows:

ISO 26262 Part 2, Clause 5.3.2:

> *5.3.2 Further supporting information*
> *5.3.2.1 The following information can be considered:*
>
> – *existing evidence of a quality management system complying with a quality standard, such as ISO/TS 16949, ISO 9001, or equivalent.*

ISO 26262 Part 2, Clause 5.4.4:

> *Quality Management during the Safety Lifecycle*
> *The organizations involved in the execution of the safety lifecycle shall have an operational quality management system complying with a quality standard, such as ISO/TS 16949, ISO 9001, or equivalent.*

This means, a well-organized, well-established and well-applied quality management system is the basis of functional safety. ISO TS 16949 is required of all vehicle manufacturers worldwide. Quality management systems without this can be disregarded. ISO 26262 also mentions several work-products where safety aspects, enhancements, or improvements need to be added to already consider work-products defined by the quality management system.

In further additions ISO TS 16949 provides the following definition for quality:

ISO TS 16949, addition:

Quality is defined as "the sum of characteristics of an entity regarding its suitability to fulfill defined and predetermined requirements". The term "entity" is here very vague. It is defined as follows: "Something that can be described and observed individually." Thus quality refers to characteristics and features of a finished product. In general it is assumed that these characteristics remain for a certain time after the production. Often this time period equals the warranty period. As long as it is stated in the specifications that the existing characteristics and features after the production should remain through the defined usage period, reliability is a part of quality.

This definition clearly asks for the concept of lifecycles as a requirement, hence quality features such as safety should be self-evident.

2.3 Advanced Quality Planning

ISO TS 16949 can be interpreted differently for the individual cases of application. This is why automobile manufacturers have since defined standards in order to guarantee quality in product development. Later, the American manufacturers such as Ford, GM or Chrysler met at AIAG to define joint requirements for quality management. In Germany, similar standards and requirements were developed under the umbrella of VDA. The aim was to define processes for the development as well as planned advanced product quality improvement measures, APQP (advanced product quality planning according to AIAG).

VDA and AIAG published a series of documents, which are considered to be the foundation for VDA- or AIAG members. Those various volumes of these documents are often mandatorily referenced in the contract documents for supplier.

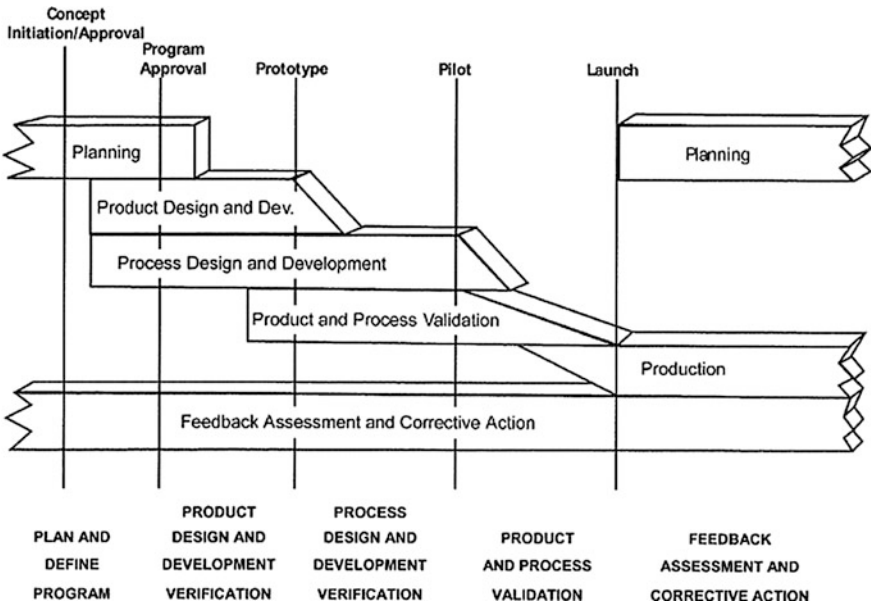

Fig. 2.5 Advanced product quality planning (*Reference* APQP AIAG [9] 4th Edition)

Unfortunately, these documents are not highly consistent. For example, both organizations describe different FMEA methods (or several FMEA methods), which are considered to be a basis of ISO 26262. In addition, these organizations also developed milestones or maturity level concepts, which were primarily used for the synchronization of automotive manufacturers and supplier (Fig. 2.5).

AIAG defined APQP with 5 "milestones":

- The first phase "Concept, initiation, approval" is a mere planning phase
- In the second phase, before the program approval, the planning as well as the product and process development should have a certain maturity. The feasibility of the product is then verified as part of the program approval.
- The third phase focuses on the development of the first prototypes, the verification (often prototype tests) and the product and production process validation. At this point, the product design should be almost finalized.
- In the fourth phase the first series-development (close-to-series-production, pilot) products are produced. Those products should already be produced with the series-production tools.
- The product launch initiates the series production. This requires the development of supply chains and the production needs to be able to guarantee a sufficient quantity and quality.

After the product launch an assessment of the product development and appropriate corrective actions are expected. All activities are continuously

monitored and necessary corrective actions need to be implemented when field findings arise.

Within this topic VDA published the following volumes:

- *VDA QMS Volume 1*
  Documentation and Archiving—Code of practice for the documentation and archiving of quality requirements and quality records/3rd edition 2008
  Guidelines for documentation and archiving of quality requirements and records (especially for critical features).
- *VDA QMS Volume 2*
  Quality Assurance for Supplies Production process and product approval PPA, 5th revised edition, November 2012
  Choice of suppliers, quality assurance and agreements, production process and product approval, choice of ingredients (A new edition will be published soon)
- *VDA QMS Volume 3, part 1*
  Ensuring reliability of car manufacturers—Reliability Management/3rd edition 2000
- *VDA QMS Volume 3 part 2*
  Ensuring reliability of car manufacturers and suppliers—Reliability Management Methods and Utilities/3rd edition 2000, currently 2004
- VDA QMS Volume 4 Chapter Product and Process FMEA [4]
  2nd edition December 2006, updated in June 2012, (The chapter is already included in Volume 4)

These volumes are continuously updated and include new topics such as maturity level of products and processes, standardized requirement specifications etc.

2.4 Process Models

Procedure or process models have a long history. The following list shows the origin of such products, especially software-intensive products.

1. First attempt to develop clearly understandable programs (1968)
   Dijkstra suggests "structured programming" (Avoidance of GOTO-instructions).
2. Development of software engineering principles (1968–1974)
   Theoretical basics (principles) are developed that represent the foundation of structured development of programs: structured programming, step-by-step refining, secrecy concepts, program modularization, software lifecycles, entity relationship model, and software ergonomics
3. Development of phase-specific software engineering methods (1972–1975)
   Implementation of software engineering concepts in draft methods: HIPO, Jackson, Constantine method, first version of small talk

4. Development of phase-specific tools (1975–1985):
   Application of SE-methods with mechanic support (e.g. Program inversion, batch tools)
5. Development of phase-comprehensive (integrated) software engineering methods (since 1980)
   The results of one phase of the software lifecycle should be automatically passed on to the next phase: integrated methods
6. Development of phase-comprehensive (integrated) tools (since 1980)
   Application of databases as automatic interfaces between the individual phases of a software lifecycle. Interactive program cue through CAS-tools (computer aided software design)
7. Definition of different, competing and object oriented methods (since 1990)
   Various object oriented analyses and design methods were developed simultaneously. (Booch, Jacobson, Rumbaugh, Shlaer/Mellor, Coad/Yourdon et al.)
   These methods were implemented with CASE tools (computer aided software engineering)
8. Integration of OO-methods for UML-unified modeling language (since 1995)
   Jacobson, Booch and Rumbaugh joint to develop UML. UML aims to eliminate the previous weaknesses of OO-methods and create an internationally valid and uniform standard. UML 1.0 passed 1997.
9. UML 2.0
   UML 2.0 was published in 2004 after UML 1.0 was upgraded to version 1.5. This version includes adapted up to date language elements for new technologies and removed redundancies and inconsistencies in language definitions.
   Source: Online list without sources

History shows, that these approaches are merely based on experience. Over time, restrictions in the programming process have led to formalized description formats. Later, the description of these "best practices" as formalized activities lead to the development of process models as reference models or, as the example of UML shows, formalized description language. Certain principles such as, requirements are only accepted if they can be implemented and if tests show that they can be implemented correctly, influenced this strategic approach.

2.4.1 V-Models

The following figure shows the development of process models and process improvement models such as CMM or SPICE. ISO 9001 and ISO 12207 can be seen as a basis for these models. ISO 12207 is mentioned in the bibliography of ISO 26262. However, the relation between ISO 12207 and ISO 26262 is not explained.

Surprisingly, for a long time the principles of the process approach for product development have not been strongly developed in Asia. ISO 12207 is the foundation of process assessment models (PAM) based on CMM or SPICE. The practice of

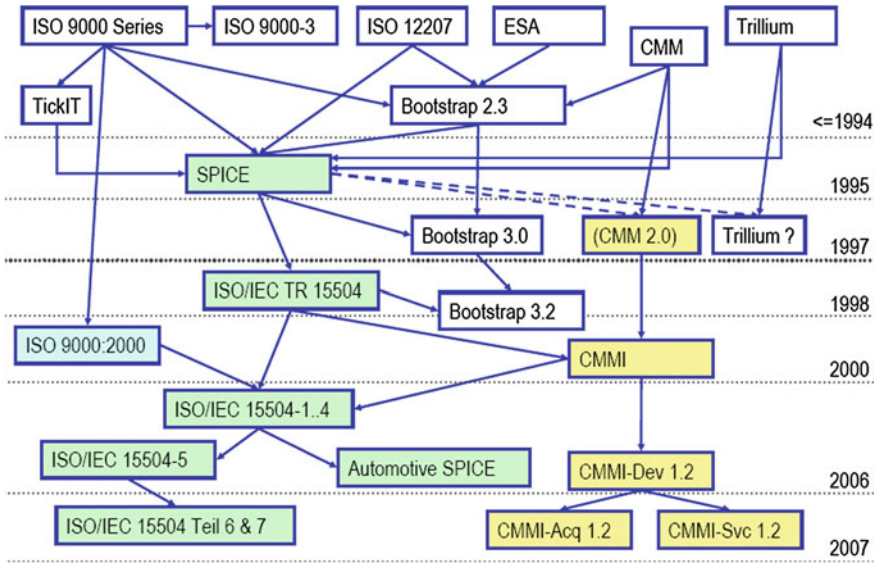

Fig. 2.6 History of procedure models based on V-models based (*Source* Flecsim)

relating those process assessment models with the safeguarding of software features was developed later.

The crucial question is 'does such a generic process actually represent more than what the SPICE-definitions describes?' Here the V-model is mentioned as a reference model. So if requirements of the development activities are described, is it useful to structure them according to such a reference model? (Fig. 2.6).

The V-model XT, in its version 1.2, describes the V only for the development of individual products (Fig. 2.7).

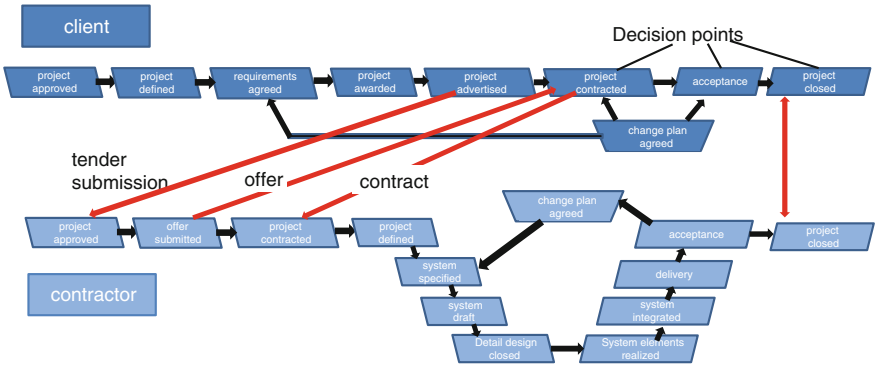

Fig. 2.7 Interface V-model customer—supplier according to V-model XT (*Source* V-model XT 1.2 [8])

The V-model XT first describes the customer—supplier relationship. This phase determines the product scope and the fundamental requirements and is comparable to part 8, Chap. 5 (Interfaces of the distributed development). Here the author refers to the interface agreement (DIA, Development Interface Agreement) between development partners. Those agreements should determine who is responsible for the various product development packages (or product elements) and who performs which activity (who does what).

SPICE (Software Process Improvement and Capability Determination) is often associated with ISO 26262 and is mainly based on two norms, ISO 12207 and ISO 15504.

ISO 12207 "Processes in software lifecycles" offers a process reference model with the following categories:

- customer-supplier processes,
- development processes,
- supportive processes,
- management processes,
- organization processes.

Part 6 of ISO 26262 mentions ISO 12207 in the bibliography appendix but there is no reference or explanation as to what relation those norms have with each other.

However, 40 processes are described, these are seen as a foundation for SW based product development and ISO 15504 derived a process assessment model (PAM) from this description.

ISO 15504 consists of the following parts:

ISO 15504-1: Concepts and vocabulary
Terms and general conception
ISO 15504-2: Implementation of assessments

- requirements for a process reference model
- requirements for PAM
- definitions of a framework to measure process capability levels
- requirements for an assessment process framework

ISO 15504-3: Guideline for the assessment implementation
Guideline for the implementation of a ISO 15504-2 conform assessment:

- Assessment framework for process capability levels
- PRM and PAM
- Selection and usage of assessment tools
- competence of assessors
- examination of compliance

ISO 15504-4: Guidelines for the usage of assessment results

- Selection of PRM
- Setting target capability

- definition of assessment inputs
- Steps to process improvement
- Steps to the determination of ability levels
- Comparability of assessment outputs

ISO 15504-5: Exemplary process assessment model (PAM)

Exemplary PAM, which fulfills all requirements of ISO 15504-2, and information on assessment indicators

ISO 15504-6: Exemplary PAM ISO 15228

- Structure of PAM
- Process performance indicators
- Process ability indicators

ISO 15504-7: Guidelines for the determination of the maturity level of an organization

CMMI and SPICE always differed in their assessments. SPICE always assesses individual processes but was unable to measure the maturity level of an organization like CMMI does. CMMI combines certain processes and therefor derives a maturity level for organizations.

With ISO 15504-7 also SPICE supports maturity levels for organizations.

ISO 15504-8: Exemplary process assessment model (PAM) for ISO 20000

Exemplary PAM for the IT service management

ISO 15504-9: Process profile goals

Part 9 is a technical specification (TS) which describes process profiles.

ISO 15504-10: Safety Extensions

Aspects of safety

AutoSIG used ISO 15504 as a basis for Automotive SPICE®. Part 2 and 5 were used for PAM and PRM. Automotive SPICE® is an adaption of parts of ISO 15504 to automotive applications.

Further lifecycle approaches for the SW development:

- ISO/IEC/IEEE 16326 Systems and software engineering—Lifecycle processes—Project management (2009)
- SAE J2640, General Automotive Embedded Software Design Requirements (April 2006)
- IEEE STD829, Standard for Software and System Test Documentation (2008)
- ISO/IEC 9126 Software engineering—Product quality (2001)
- ISO/IEC 15288 Systems engineering—System lifecycle processes (2002)
- ISO/IEC 26514 Systems and software engineering—Requirements for designers and developers of user documentation (2008)

All these norms influenced the development of ISO 26262. However, none of these norms from the list above is in a normative relationship with ISO 26262.

However, the norms of the ISO/IEC 25000 [5] were highly influential. They were developed simultaneously to ISO 26262 and since 2005 have replaced ISO/IEC 9126.

The basic norm is called:

ISO/IEC 25000 Software engineering—Software Product Quality Requirements and Evaluation (SQuaRE)

This series includes quality criteria and the ISO organization asks other norm developing working groups to use these as guidelines.

The following examples show a comparison of the definitions of ISO/IEC 25000 and ISO 26262:

Functionality:

The capability of the software product to provide functions, which meet stated and implied needs when the software is used under specified conditions.

Generally does not contradict with ISO 26262

Functional appropriateness:

Degree to which the functions facilitate the accomplishment of specified tasks and objectives. EXAMPLE An user is only presented with the necessary steps to complete a task, excluding any unnecessary steps.

NOTE Functional appropriateness corresponds to suitability for the task in ISO 9241-110.

The term is not used in ISO 26262, but does not mean any contradiction.

Functional correctness:

Degree to which a product or system provides the correct results with the needed degree of precision.

Considered as part of verification measures, but not addressed as such in ISO 26262.

Interoperability:

Degree to which two or more systems, products or components can exchange information and use *the information that has been exchanged*

NOTE Based on ISO/IEC/IEEE 24765.

The focus in ISO 26262 lies more on the flawed cooperation of elements and systems.

The term is not used in ISO 26262, but does not mean any contradiction.

Security:

Degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization.

NOTE 1: As well as data stored in or by a product or system, security also applies to data in transmission.
NOTE 2: Survivability (the degree to which a product or system continues to fulfill its mission by providing essential services in a timely manner in spite of the presence of attacks) is covered by recoverability (4.2.5.4).

NOTE 3: Immunity (the degree to which a product or system is resistant to attack) is covered by integrity (4.2.6.2).
NOTE 4: Security contributes to trust (4.1.3.2).

The term is not yet addressed, but it is a big topic for future revisions of ISO 26262.

Authenticity:

Degree to which the identity of a subject or resource can be proved to be the one claimed

NOTE Adapted from ISO/IEC 13335-1:2004.

The term is not used in ISO 26262, but does not mean any contradiction.

Reliability:

Degree to which a system, product or component performs specified functions under specified conditions for a specified period of time

NOTE 1: Adapted from ISO/IEC/IEEE 24765.
NOTE 2: Wear does not occur in software. Limitations in reliability are due to faults in requirements, design and implementation, or due to contextual changes.
NOTE 3: Dependability characteristics include availability and its inherent or external influencing factors, such as availability, reliability (including fault tolerance and recoverability), security (including confidentiality and integrity), maintainability, durability, and maintenance support.

The term is not used in ISO 26262, but does not mean any contradiction. But this book will address more the relation between safety and reliability.

- *Maturity: Degree to which a system, product or component meets needs for reliability under normal operation*

NOTE: The concept of maturity can also be applied to other quality characteristics to indicate the degree to which they meet required needs under normal operation.

The term is not used in ISO 26262, but does not mean any contradiction.

- *Fault tolerance: Degree to which a system, product or component operates as intended despite the presence of hardware or software faults*

NOTE Adapted from ISO/IEC/IEEE 24765.
Reliability is used in a comparable context but also for software and hardware.

The term is not used in ISO 26262, but does not mean any contradiction.

Recoverability:

Degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system.

NOTE: Following a failure, a computer system will sometimes be down for a period of time, the length of which is determined by its recoverability.

The term is not used in ISO 26262, but does not mean any contradiction.

Compliance:

Extend to which the software fulfills reliability norms and agreements

ISO 26262 compares and refers compliance especially to safety.

Usability:

Degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

NOTE 1: Adapted from ISO 9241-210.
NOTE 2: Usability can either be specified or measured as a product quality characteristic in terms of its sub characteristics, or specified or measured directly by measures that are a subset of quality in use.

The usability of for example components describes the qualification of components in safety applications.

Efficiency:

Resources expended in relation to the accuracy and completeness with which users achieve goals [ISO 9241-11]

NOTE: Relevant resources can include time to complete the task (human resources), materials, or the financial cost of usage.

Efficiency is especially reference to the efficiency of safety mechanism in ISO 26262.

- *Time behavior: Degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements*

Real-time aspects are not directly addressed, but safe tolerance time interval or any other time related requirements define constraints for safety-related functions.

- *Resource utilization: Degree to which the amounts and types of resources used by a product or system, when performing its functions meet requirements*

NOTE: Human resources are included as part of efficiency (4.1.2).

Resource usage of microcontroller is a major topic in safety engineering, but not addressed in detail in ISO 26262.

Maintainability:

Degree of effectiveness and efficiency with which a product or system can be modified by the intended maintainers

NOTE 1: Modifications can include corrections, improvements or adaptation of the software to changes in environment, and in requirements and functional specifications. Modifications include those carried out by specialized support staff, and those carried out by business or operational staff, or end users.
NOTE 2: Maintainability includes installation of updates and upgrades.
NOTE 3: Maintainability can be interpreted as either an inherent capability of the product or system to facilitate maintenance activities

ISO 262626 does not make a focus on maintainability a for example railway safety standards, but the relation between safety and maintenance is addressed.

- *Analyzability: Degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified*

  NOTE: Implementation can include providing mechanisms for the product or system to analyze its own faults and provide reports prior to a failure or other event.

  The term is not directly addressed, but safety analyses are key activities for element examinations of the product under development.

- *Modifiability: Degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality*

  NOTE 1: Implementation includes coding, designing, documenting and verifying changes.
  NOTE 2: Modularity (4.2.7.1) and analyzability (4.2.7.3) can influence modifiability.
  NOTE 3: Modifiability is a combination of changeability and stability.

  The term is not used in ISO 26262, but does not mean any contradiction. Especially changeability is seen more specifically in the context of a supportive process (Change management).

- *Stability: Probability of the occurrence of unexpected impacts or changes.*

  The term is not used in ISO 26262, but does not mean any contradiction

- *Testability: Degree of effectiveness and efficiency with which test criteria can be established for a system, product or component and tests can be performed to determine whether those criteria have been met.*

  NOTE: Adapted from ISO/IEC/IEEE 24765.
  It is considered in the same context by using tests a verification measure.

- *Compliance: Extend to which the software fulfills norms and agreements in reference to changeability.*

Confirmation Measure require, questioning or examine compliance to ISO 26262.

Portability:

Degree of effectiveness and efficiency with which a system, product or component can be transferred from one hardware, software or other operational or usage environment to another

NOTE 1: Adapted from ISO/IEC/IEEE 24765.
NOTE 2: Portability can be interpreted as either an inherent capability of the product or system to facilitate porting activities, or the quality in use experienced for the goal of porting the product or system.

The term is not used in ISO 26262, but does not mean any contradiction

- *Adaptability: Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments*

NOTE 1: Adaptability includes the scalability of internal capacity (e.g. screen fields, tables, transaction volumes, report formats, etc.*).*
NOTE 2: Adaptations include those carried out by specialized support staff, and those carried out by business or operational staff, or end users.
NOTE 3: If the system is to be adapted by the end user, adaptability corresponds to suitability for individualization as defined in ISO 9241-110.
The term is not used in ISO 26262, but does not mean any contradiction

- *Install ability: Degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment*

NOTE: If the product or system is to be installed by an end user, install ability can affect the resulting functional appropriateness and operability.
The term is not used in ISO 26262, but does not mean any contradiction

- *Co-existence: Degree to which a product can perform its required functions efficiently while sharing a common environment and resources with other products, without detrimental impact on any other product*

Co-existence of function and especially software with different ASIL within common elements addresses the ability of co-existence of the different elements in common resources and its different ASIL.

- *Replace ability: degree to which a product can replace another specified software product for the same purpose in the same environment*

  NOTE 1: Replace ability of a new version of a software product is important to the user when upgrading.

NOTE 2: Replace ability can include attributes of both install ability and adaptability. The concept has been introduced as a sub characteristic of its own because of its importance.
NOTE 3: Replace ability will reduce lock-in risk: so that other software products can be used in place of the present

The term is not used in ISO 26262, but does not mean any contradiction

Those ideas and terms are illustrated in ISO 26262 in a different or similar context. For example coexistence of software of different criticality (different ASIL) doesn't see a risk if functions are similar but if these functions can influence each other negatively. Furthermore, it is important to mention that ISO 26262 uses and defines the terms validate, verify, analyze, audit, assessment and review in context of functional safety for road vehicles differently. These examples also show that requirements, terms or definitions within ISO 26262, depending from which activity or context they are used, can lead to different interpretations or meanings.

Furthermore, there are two basis process models, which need to be considered in order to observe the valid variance of processes in the development according to ISO 26262.

2.4.2 Waterfall Model

The waterfall model is a process model often found in the development of tools (Fig. 2.8).

This model has no specific source of origin. This is why there are so many different descriptions and interpretations as to how this model can be applied. The waterfall in general describes a higher level of abstraction than most V-models.

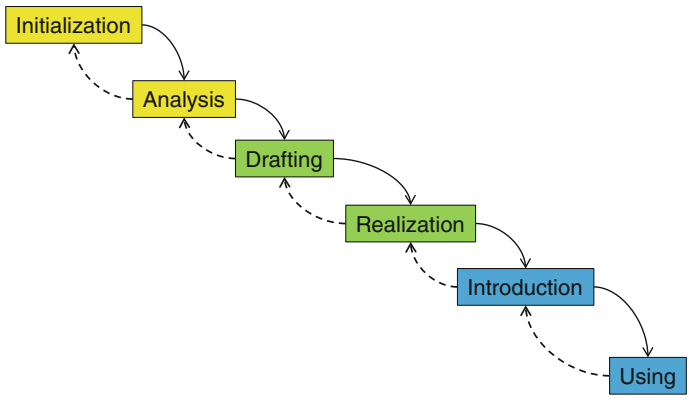

Fig. 2.8 Waterfall model [6] (*Source* Wikipedia)

Furthermore, to better picture the process one can imagine that the waterfall model transforms into a V-cycle for the design and implementation phase. Compared to waterfall models, V-based process models describe vaster parts of lifecycles. All other process models describe the initialization phase as a linear starting point that defines the interests (stakeholders, see chapter "Stakeholders of an architecture") or sources of requirements (compare to SPICE: "Requirement Elicitation") for a system.

The introduction and application right up until the product definition or the contract document and the requirement specification are often described as a linear path in process models. Iterations are not further evaluated in later phases. In addition, iterations of the planning and defining activities between the customer and the service provider are not necessarily included in the development activities.

This shows that most of the process models are derived from the IT world. A derivation of the waterfall model for the automobile industry would certainly resemble parts of the safety lifecycle of ISO 26262 or the various APQP standards.

2.4.3 Spiral Model

More often, the V-model is also discussed in regards to automotive industry. However, the traditional process model in this sector seems to be the spiral model.

As mentioned in the chapter 'Advanced Quality Planning', sample phases mainly determine the development activities in the automobile industry. The following figure shows the sequential process and the respective iterations in a spiral shape (Fig. 2.9):

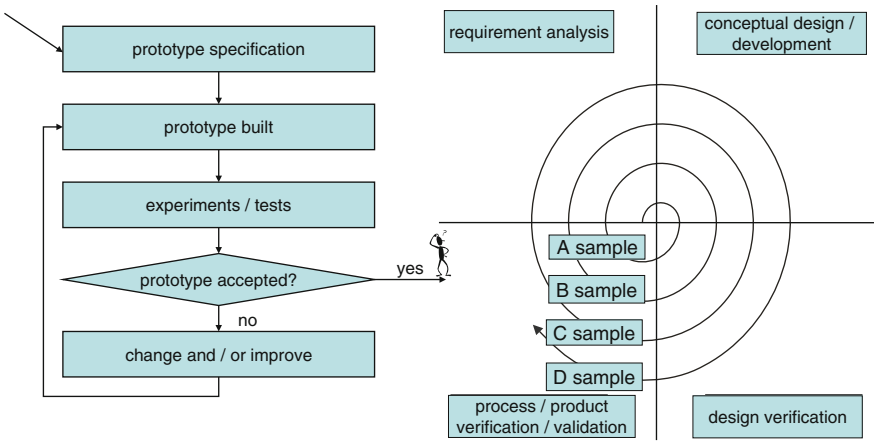

Fig. 2.9 Spiral model for a prototype- or sample-cycle approach as basis for many automotive maturity models

Today, traditional sample names such as A-, B-, C- and D-sample are only referenced in certain company standards (e.g. in Daimler's). In the APQP standards from AIAG or VDA all samples refer back to the initial sample. The sample groups for different customers are mostly aligned with the requirements of the vehicle development.

Phases of the Spiral: Prototypes

The dream of every process developer is that specification actually represents the beginning of product development. In reality, it is more an idea, which has to be built up for series production. For classic mechanics it is a trial sample that has to be complemented with essential functions or electrified for new systems. Therefore, there is often only one specification, which is defined on a higher level of abstraction in the first iterations.

Previously, in the early stage of automobile engineering, the A-sample could be made out of wood since the main focus at the beginning was the production potential of the inside of the vehicle. Today, in modern systems, the first step can already focus on the entire outer interface, so that the CAN-communication can already be adjusted to the target vehicle in the first sample delivery.

Construction of Prototypes

Since samples have to be delivered to the customers, they have to be produced in the first place. Certainly, this requires a lot of manual work in the first iterations. In the following iterations the degree of automation increases continuously. Then, the D-Sample—often comparable to the first sample/initial sample—has to be produced in the series production facility.

Experimenting—Trial/Acceptance

Moving forward, the sample has to be tested according to the given requirements. The sample will be tested in the first iterations First under laboratory conditions, and then later based on with the customer requirements, and in further stages often already in the vehicle environment in order to explore the dynamic behavior as well as the interaction of all components.

All parties involved in the process hope to be able to figure out all necessary requirements in the first shot and that the sample returns with a positive test result. In the real world, the prototype is an essential input factor for the requirement analysis. Besides simulation, this method has also been adopted in ISO 26262.

Changes, Modifications or Enhancements

Here the specifications are now changed and the new specifications introduce a new development cycle.

With DRBFM (Design Review Based on Failure Mode) Toyota was very early to develop a stable method, which introduces new iterations. Whether a specification is complete or still error-prone is difficult to examine (freely adapted from Popper: verification is positive until I can find a counterproof). Change

management based of specifications can only be effective if it is known whether the specification is correct and clearly and distinctively valid for the product. Pessimists would say that this is impossible. This is why DRBFM describes a comparison based on features. In a multidisciplinary team, features are compared to functional dependencies (architecture). The positive and negative influence on a product is analyzed and assessed in a design review before proposals for modifications are accepted. This method is very useful for modern architectural developments.

The result of DRBFM is only adopted for the specification after the effects analysis and is then accepted as a modification for the product.

These aspects also influenced change management processes and requirements in ISO 26262.

2.5 Automotive and Safety Lifecycles

IEC 61508 was probably the first standard that described a safety lifecycle. The vastly simultaneously developed ISO/IEC 12207 also described a software lifecycle. It was discovered in the mid 90s that the requirements of a product could influence its design over the entire usage period. Unfortunately, it was also known that certain mistakes in all phases could lead to danger and people could get injured while dealing with certain products. ISO/IEC 12207 shows that there is a demand for the monitoring of specific error patterns of products throughout all phases of the product lifecycle. Those error patterns present further challenges for the design of a product.

The APQP standards also consider early development phases. The terms of the System-FMEA as well as later design or concept-FMEA are included in the norms. Product maintenance and the management of replacement parts have been considered by the APQP norms for quite a while. Also the idea of document archiving throughout the lifecycle has been addressed by the norms at a very early stage. The demand arose from the topic of product liability.

In IEC 61508 the lifecycle was used to define phases from the product idea up to the end of the product life, in which individual safety activities can be implemented. This lifecycle already represented the foundation to fully describe the actual requirements of a product.

Safety considerations of a product idea are already of particular importance and not only because of safety related reasons but also and most importantly economic aspects. History has shown that bad ideas sometimes can turn out to be successful. Unfortunately, bad ideas have often been pursued only because of the fear of failure and the potential hazards occurred when the possibility to prevent them no longer existed. A production stop can often cost a company more than the compensation of damages that the product might cause when used. This covers one main aspect of product liability, which has previously been addressed by the legislatures of the 19th century. For example, §823 of German civil law requests to avoid hazards of products as far as science and engineering will allow it. Also, the retailer or distributor of goods is liable for damages occurred.

Let's get back to the product and safety lifecycle. A function can cause a hazard even if it operates as intended. This is mainly referred to as safety-in-use. As mentioned in earlier chapter (safety, risk etc.) this is not addressed in ISO 26262. However, the hope is to find something throughout the course of product development that can manage the risk. Otherwise, the respective functions are limited as much as possible in order to eliminate risk.

ISO 26262 can only help to control hazards based on a malfunction of the product. Experienced engineers might be able to find safety mechanisms for dangerous functions. If those mechanisms are not found the product has no chance to establish itself on the market. It can be a real challenge to sufficiently declare such defects/faults/errors as unlikely for complex products that are produced in high quantities. Formally, the quantification of those systematic errors are not required by ISO 26262. The characteristics of such complex products, their potential errors as well as the potential variance of their usage are hard to determine. The product might still be able to enter the market but once the first hazard arises the only option is to withdraw it from sales and recall the entire vehicle. It has previously occurred that some manufacturers have had to buy back vehicles. This is why one of the first steps in order to get to the field of application of ISO 2626 is to prove the safety of use/usage safety of the product. In order to avoid potential liability issues, it is useful to clearly document all safety issues to prevent safety-in-use being questioned after certain changes are made during the following development. Generally, the nature of an engineer is not to scrap an idea after the first failure but to adapt and modify it accordingly.

In order to take a brief look at the end of the product lifecycle, let's discuss certain aspects of the product lifecycle itself. In regard to hazards, the public discussion on mobile phones would be a good example.

Of course, a lot of qualitative electrical waste is produced due to the fast and short lifecycles of electronic products. This wouldn't be questionable from a safety perspective if the components themselves were not so expensive and were not environmentally damaging materials, such as lead. This is why the government implemented clear procedure rules. Now it may be far-fetched to say that the toxic electrolytes in capacitors may also eventually cause environmental damage or that the burst of an electrolyte capacitor is a malfunction of an E/E element.

But the question here is whether or not ISO 26262 is helpful in this regard. In fact, there is a potential for hazards that have to be considered in the production and development of products, to prevent issues with product liability. In cases such as these, it is important to consider the possible end of a sub product. In general, cars are used beyond their actual warranty. Cars that are over 25 years old can possibly become classic/vintage cars and more popular than a car with the latest engineering technology. Luckily, cars made 25 years ago used far fewer electronics. However, this will now change from year to year. It is particularly important to consider the maintenance of the car, particularly those components and systems that are subject to wear and tear.

Opel once advertised with a lifelong warranty, meaning 15 years and 160,000 km (99,419.3908 miles)—a campaign that was quickly abolished. We also

learned that NASA bought Intel's 8086 microcontrollers via eBay in order to be able to maintain old systems. It is increasingly difficult nowadays to maintain program parts written in FORTRAN. Such dated systems are practically impossible to re-lay with systems such as WINDOWS and other advancing computer systems. Going forward, we will see that a prognosis for an electrical component beyond the failure mode of more than 10 years is extremely difficult. Nowadays, in the field of utility, vehicles lifespans of over 20 years are projected. Intermittent errors have already been detected in an 8086 but it is highly questionable whether actual measures in the integration have been undertaken.

To assure maintenance according to safety aspects will become a real challenge for the automobile industry.

2.5.1 *Safety Lifecycles for the Development of Automotive Products*

ISO 26262 describes safety lifecycles in part 2, Chap. 5 "Overall Safety Management". Here, the idea is to inter-relate safety lifecycles, product lifecycles and the "Management of Functional Safety". The aim of the management of functional safety according to ISO 26262 is to define the responsibility of acting individuals, departments and organizations that are responsible for each individual phase of the safety lifecycle. This applies to necessary activities, functional safety for products, and the vehicle system—or as referred to in the norm—the ITEM, as well as measures must be taken in order to confirm that the products are developed according to ISO 26262 guidelines.

Moreover, other activities have to be described that are necessary and important beyond the safety lifecycle in order to show a respective and appropriate infrastructure in order to apply the product lifecycle. Very important here is an applied and utilized quality management system and safety culture to ensure that each individual employee, right up to the top management regard safety with the required diligence and respect in order to implement and apply the necessary measures appropriately. Further crucial premises are the systematic learning process from previous mistakes, competence management and continuous improvement such as qualification and training programs in order to apply a safety lifecycle.

ISO 26262 generally assumes that products are developed within a project structure. Here there is a chance that divisions or organizations develop products according to a general interpretation or implementation of a product lifecycle ("Project independent tailoring of the safety-lifecycle"). This means a process scope is developed, that represents a valid derivation of ISO 26262 but can also be optimized in regards to infrastructure and product aspects.

Alternatively, each product development can be directly derived from the scope of ISO 26262 as for example as project safety plans. Especially in product development and production it can be favorable to define many activities—customer and/or product alike. This can be of advantage in machinery utilization or in the

scope of product development. Internal processes can be coordinated and aligned appropriately to qualified development tools and different versions for various customers can be offered with little effort. Also, the reuse of established processes, safety components or products can have a positive effect on the safety of all products.

2.5.2 *Safety-Lifecycles According to ISO 26262*

The safety-lifecycle of ISO 26262 summarizes the most important safety activities in the conceptual phase, the series production and the series production release. A central management task is the planning, coordination and proof of these activities throughout all phases of the lifecycle. Volumes 3, 4 and 7 describe the activities of the conceptual phase, the series production and those according to SOP thoroughly (Fig. 2.10).

This safety-lifecycle directly refers to the respective chapter in ISO 26262. The management of functional safety according to part 2 of the norm includes all further activities from part 3 (Concept Phase) to part 7, Chap. 6 (Operation, service (maintenance and repair), and decommissioning)

The safety-lifecycle is divided into 3 phases:

- Concept
- Product development
- After production release/approval

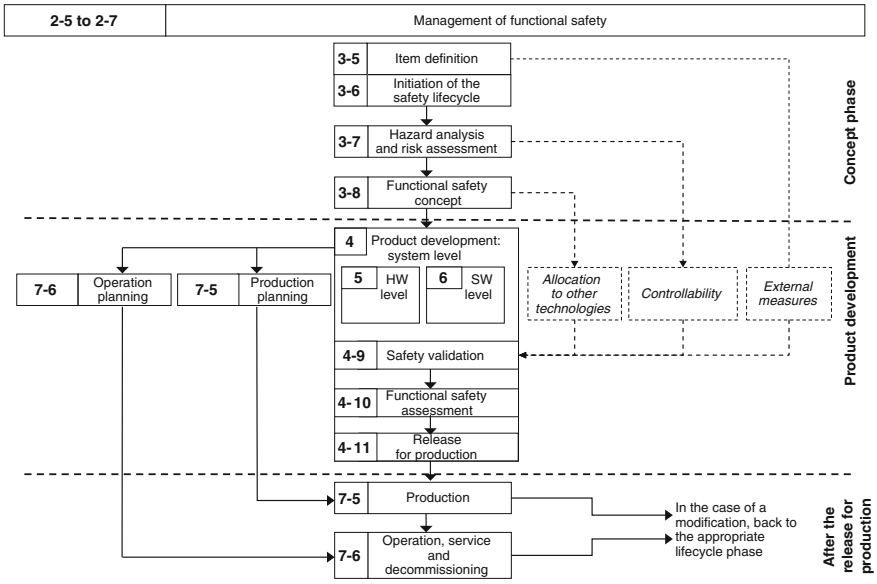

Fig. 2.10 Safety-lifecycle according to ISO 26262 (*Source* ISO 26262, part 2)

Please note that the technical safety concept is associated with the product development. Next to the 3 parts of product development of systems, EE-hardware and software, and the chapters about production development and plant engineering (part 7) are described. Those are activities that are considered besides the development V-cycles. Furthermore, some activities are mentioned that are not directly addressed by the norm but often necessary for the product development.

External Measures
These are measures that are not influenced by the observation unit, which are described in the system definitions. External risk reduction includes for example the behavior of road users or characteristics of the road itself. This is also described in the system definitions. External risk reduction is seen as profitable within the scope of the hazard and risk analysis. The proof of efficiency of external risk reduction is not included in this norm.

Controllability
Controllability, the underlying concept of the hazard and risk analysis, should be proven within the phase of product development. If it does not relate to the distinct controllability of individuals exposed to hazard, then it is covered in part 3 of ISO 26262. This part overlaps with the content of safety-in-use, since the question whether functions are defined in a way that they are not dangerous when functioning properly is also relevant.

Association to measures of other technologies
These are technologies that are not covered in the scope of this norm, for example, mechanics and hydraulics. They are addressed when associated to safety functions. Also, the proof of efficiency or effectiveness and even the application of these measures are not part of this norm.

In the scope of the functional safety management the norm requires certain activities for the safety-lifecycle:

- Sufficient information has to be documented to the E/E-system for each phase of the safety-lifecycle, this is necessary for the effective fulfillment of the following phases and verification activities.
- Management of functional safety has a duty to ensure the execution and documentation of phases and activities of the entire lifecycle and to provide a corporate culture that promotes functional safety.

From the point of view of functional safety it is not about the fulfillment of the requirements that are derived from any process models. The safety-lifecycle has to be derived correctly and sufficiently. It is important for project planning and the planning of safety activities that the safety concepts are implemented in a way that sufficiently ensures safety goals.

2.5.3 *Security-Versus Safety Lifecycles*

For meaningful safety-related product development not any quality characteristics could apply their own process. Therefor also even if there are other means of analysis or methods for verification or validation necessary, it is a matter of tailoring of the product lie-cycle to apply activities to as necessary for all non-functional requirements also such as security. Similar to challenges with the safety lifecycle for safety-related active safety functions and other passive safety functions the tailoring and even the entry into the safety lifecycle is different. The intended safety function for an active safety function should be made safe by adequate measures during the Item Definition, and for typical passive safety functions it should be done during entire safety lifecycle.

Mayor security threads are categorized as follow:

- Availability
  Assures access to data and infrastructure
- Integrity
  Identification of manipulation of data on controller or communications
- Confidentiality
  No unauthorized information access

A particular security topic is theft-protection, since this provides many dependent functions to Functional Safety.

Furthermore, all "Integrity" related issues are very often also causes for "Functional Safety" impacts.

References

1. [ISO 26262]. ISO 26262 (2011): Road vehicles – Functional safety. International Organization for Standardization, Geneva, Switzerland.

ISO 26262, part 3, appendix B1:	11
ISO 26262 Part 2, Clause 5.3.2:	17
ISO 26262 Part 2, Clause 5.4.4:	18

2. [IEC 61508]. IEC 61508 (2010): Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission, Geneva, Switzerland.

IEC 61508, Part 1, Part 5, A5:	9

3. [ISO TS 16949]. ISO/TS 16949 (2009): Systems. Particular Requirements for Application of ISO 9001:2008 for Series- or Spare parts Production in Automobile industry; VDA, 3rd English edition 2009.

4. [VDA FMEA] VDA (2008), Volume 4 Chapter, Product and Process FMEA, QMC, Berlin 20
5. [ISO/IEC 25000]: ISO/IEC 25001:2007, Software engineering—Software product Quality Requirements and Evaluation (SQuaRE) — Planning and management 25
6. [waterfall model]: Figure 2.8: Waterfall Model (Source: Wikipedia) 30
7. [unpublished research project], for further information available
8. [V-model XT 1.2], V-Modell® XT, Version 1.2.1.1, IABG, 2008
9. [APQP AIAG], APQP AIAG 4th Edition, Automotive Industry Action Group, APQP, 2006

http://www.springer.com/978-3-319-33360-1

Functional Safety for Road Vehicles
New Challenges and Solutions for E-mobility and Automated Driving
Ross, H.-L.
2016, XV, 269 p. 128 illus., 101 illus. in color.,
Hardcover
ISBN: 978-3-319-33360-1