Reliability Assurance of Subsea Production Systems: A Systems Engineering Framework

Sirous Yasseri[1], Hamid Bahai[2], Ramin Yasseri[3]

[1]PhD Brunel University London; Sirous.Yasseri@Brunel.ac.uk
[2]Professor, Brunel University London; Hamid.Bahai@Brunel.AC.Uk
[3]MSc Systems engineer Aker Solution London; Ramin.Yasseri@gmail.com

ARTICLE INFO	ABSTRACT
	Due to the high investment costs for deep-water subsea production systems of high-value subsea fields, it is crucial to ensure a high availability to recover the investment. The problem is compounded by the cost of recovery, repair and replacement of failed equipment. Testing and reliability analyses are two pillars of reliability assurance; neither of them on their own assures the delivery of a reliable system. Possibly with more imaginative use of reliability methods, it is possible to optimise testing. It is suggested to use reliability analysis as a guide for allocating resources for testing. This paper outlines a Systems Engineering Framework to link the Client's requirements for equipment reliability, as a means of proving the desired level of performance. This framework allows a better understanding of verification settings and strategies to handle constraints (e.g. costs, expandability, repair-ability, maintainability, intervention procedures, downtime, automation etc.) and performance measures, to achieve highly reliable production systems. The bilateral links between the Client's requirements and subsea equipment performance are established using the systems engineering V-model. These links relate equipment performance to one or more of the Client's requirements, which helps establish verification and validation testing strategies to enhance reliability and reduce project risk. The proposed procedure also assists risk management efforts by feeding the results of reliability analyses, testing and project risk analysis into validation processes, the systems engineering measurement process ensures enhanced reliability. We define reliability assurance as a part of the systems engineering processes to ensure the continued function and resilience of the production system from the downhole valve to the subsea equipment, housed on the topside or at an onshore terminal, in their operating environment and condition using the "Fit-For-Service" notion.

1. Introduction

High-value subsea production systems rely on high reliability and high availability to avoid loss of revenue since access and downtime are costly. The industry needs a comprehensive and integrative framework to assess and address ways and means of achieving high availability.

The Client sets the required reliability, which is then used to allocate the reliability for each piece of hardware/software. With reliability requirements specified, the primary task is to confirm "by examination and provision of evidence that the hardware (and software) meets the specified requirements for the intended use" (DNV-RP-A203

[8]). When completely new technology is involved, available data is likely to be insufficient, which means that the confidence in the gathered evidence may not be high; thus, more testing may be necessary (Yasseri et al [41]). Reliability may also be reduced by a possible mismatch between specification, design, manufacture, installation, commissioning and use. This means that the predicted performance demonstrated through the qualification process may be different from the actual performance realized in the field. This may be due to emergent behaviour, unidentified failure modes, unanticipated operating conditions, unforeseen failure mechanisms and causes, epistemic uncertainties or aleatory

uncertainties (Pecht [30]). Unanticipated operating conditions are either due to incorrect/inadequate specifications or because of unforeseen changes in the actual well conditions. A scenario-based approach can help to minimise the effect of uncertainties. The 'provision of evidence' is done through functional failure analysis (Viola, et al [34]), and testing; supplemented by experience from proven technologies and physics-based analyses.

The key to assuring system and equipment reliability is the insight gained during the specification writing and design activities, which are used to establish procedures to control the fabrication and manufacturing processes that will result in equipment with the desired quality attributes; specifically

- Understand the sources of variation;
- Detect the presence and degree of variation;
- Understand the impact of variation on the process and hence on the equipment attributes;
- Control the variation in a manner compatible with reliability need of the equipment.

Reliability methods that focus on using historical data to predict mechanical failures imply that design errors have little impact, and assume that all anomalies will be detected during design and fabrication. But design errors offer a challenge to reliability predictions based on historical data only (Feiler, et. al [13]) because it is unrealistic to assume that what we build now is the same as we built in the past. Verification and validation testing are supposed to fill this gap. However, there is a need for a more dependable approach for qualifying a system, rather than "test it until time and budgets are exhausted". Such an approach should allow detecting problems in the Development Phase of the life cycle to assure operational quality attributes, such as performance, timing, safety, reliability, and security. Such an approach must identify defects before a system is built, as well as deal with issues that are hard to test unless the entire system is built. It is necessary to ensure that unavoidable failures are addressed through risk management, providing resilience to counter undetected and emergent behaviour.

The reliability assurance framework which is outlined in this paper utilises systems engineering processes which are generally performed for the project; two of the primary processes are:

- Requirement analysis at the system, subsystem and components levels. Systems requirements are based on the Client's needs and the concept of operation (ConOp)- see INCOSE [20]. System requirements fall into two categories; Firstly, the required capabilities under normal conditions, such as functionality, behaviour, and performance. Secondly, specifying how the system is expected to perform under abnormal conditions, such as resilience and survivability (robustness). Requirements are linked to the concept of operation (ConOp) [20] and flowed down into requirements for subsystems, assemblies and components (Hull et. al [17]).

- System architecture. The subsea industry has recognized that a high reliability starts with the system architecture, i.e. arrangement and packing of components. The architecture should allow access to equipment to be retrieved by Remotely Operated Vehicles (ROVs) with minimal effort and time. Model-based analysis, simulations and analytical approaches can be used to identify problematic areas. The subsea Industry has embraced virtual system integration to achieve validation through Computer Aided Design (CAD) modelling. Analysis of integrated systems and detailed models are used for early discovery of likely problems (Youngblood and Pace[41]).

2. Fitness for Purpose or Service

This paper uses the concept of Fitness-For-Purpose (FFP), which is also referred to as Fit-For-Service (FFS) in this paper. It can be said a system is badly designed if it is not well suited for its intended purpose, i.e. it is not fit for service. The phrase Fit-For-Service is also used in fracture mechanics literature in relation to the size of tolerable cracks. In the paper, this phrase is used to mean for whatever reason is not suitable for service. If a component is added to make the operation safer, but it does nothing, then it is not Fit-For-Purpose. Thus, quality can be defined in terms of Fitness-For-Purpose. This means that the quality cannot be assessed as a measure of the production system itself; quality can only be assessed when considering the production system in the context of what it must do. In other words, hardware on its own cannot be said to be of 'high quality' or of 'low quality', because the quality is an attribute of the relationship between hardware and the purpose for which it is used. The purpose of a system, and hence the key quality measures, appear to be self-evident. For example, it is hard to imagine a purpose for a subsea control system that does not allow shut down the system in an emergency as safely as practicable. Most systems have multiple purposes, and those purposes change over time. Thus, conditions under which a system must work, and the intended purpose, must be properly understood.

With a notion of "Fitness-For-Purpose", one can consider and challenge the comprehensiveness and relevance of purposes to ensure improvements. FFP equates quality with the fulfilment of a specification or stated goal. It attempts to validate a product for its intended use. The purpose may be that as determined by the safety, reliability and quality requirements, which are in turn based on the needs of customers. Thus, FFP is fulfilling customers' requirements, which is one of the possible criteria for establishing whether a unit meets quality, measured against what is seen to be the goal of the unit. This definition

subsumes value for money under fitness for purpose. However, affordability or cost-effectiveness criteria are not a necessary element of Fitness-For-Purpose.

Fitness-For-Purpose has emerged as the fashionable way to harness the drive for perfection, i.e. zero defects. The ultimate measure of perfection, 'zero defects', may be excellent as a definition of quality but runs the fatal risk of being perfectly impractical. If the product does not fit its purpose, then its perfection is irrelevant.

A major weakness of the FFP concept is that it may seem to imply that "anything goes" so long as a purpose can be formulated for it. This weakness is more likely to be exacerbated in a large organisation with a range of "purposes" to minimise CAPEX or/and OPEX, which are controlled by different business units. Such separation of decision makers will lead to complications in building installations in various jurisdictions with different regulations. Although straightforward in conception, "Fitness for Purpose" is deceptive, for it raises the issue of whose purpose and how fitness is assessed? Thus, this paper replaces "Fitness-For-Purpose", with "Fitness-For-Service", since while FFP is unclear FFS is obvious. FFS is assessed for the entire lifecycle (ISO/IEC 15288, 2008 [23]). In the literature on the acceptability of flaws in welded component FFS is used to mean the largest size of a crack a component can contain while can be used in service. The usage of FFS in this paper is much wide and include every type of flaw.

Proving a system's Fitness-For-Service requires gathering evidence. This involves the development of evidence in parallel with the system design throughout the Development Phase of the life cycle. Such evidence includes: requirements and design reviews,

results from the predictive analysis, simulation results and test results to provide justified confidence in the built system. This approach documents claims about the system, assumptions made in the process, and evidence required to satisfy these claims.

3. The State of Practice

Several codes of practice, as well guidance notes from the classification society have been published in recent years; e.g. API, 17N [3] & 17Q [4], DNV-RP-A203 [8], Bureau VERITAS [7], ABS [2], and Lloyds Register [25]. Figure 1 shows DNV-RP-A203 [8] procedure.

Although, these standards and guidance notes primarily address "New Technology", the definition of the new technology includes almost everything in a new site, and even includes some sites with a previous history. The term 'Technology' refers to equipment that uses a physical law to perform a function. Both equipment and its physics must be qualified. Where subsea equipment is the marinized version of topside equipment, hardly any new physics is involved, then it is the equipment only that requires qualification.

The primary method for proving the 'claim' that a piece of equipment is qualified, is by gathering valid evidence (Yasseri [40]) which proves the equipment will function within specific limits and with an acceptable level of confidence (Woody, et al [35]). This is obtained by a combination of modelling, simulation, physics-based analytical & numerical methods, reliability methods (FMECA, RAM, Reliability Block Diagrams, etc. see e.g. IAEA [14]), risk assessments and tests. API codes (API RP 17N [3], and 17Q [4]) follow a similar line with some deviation (Figure 2).
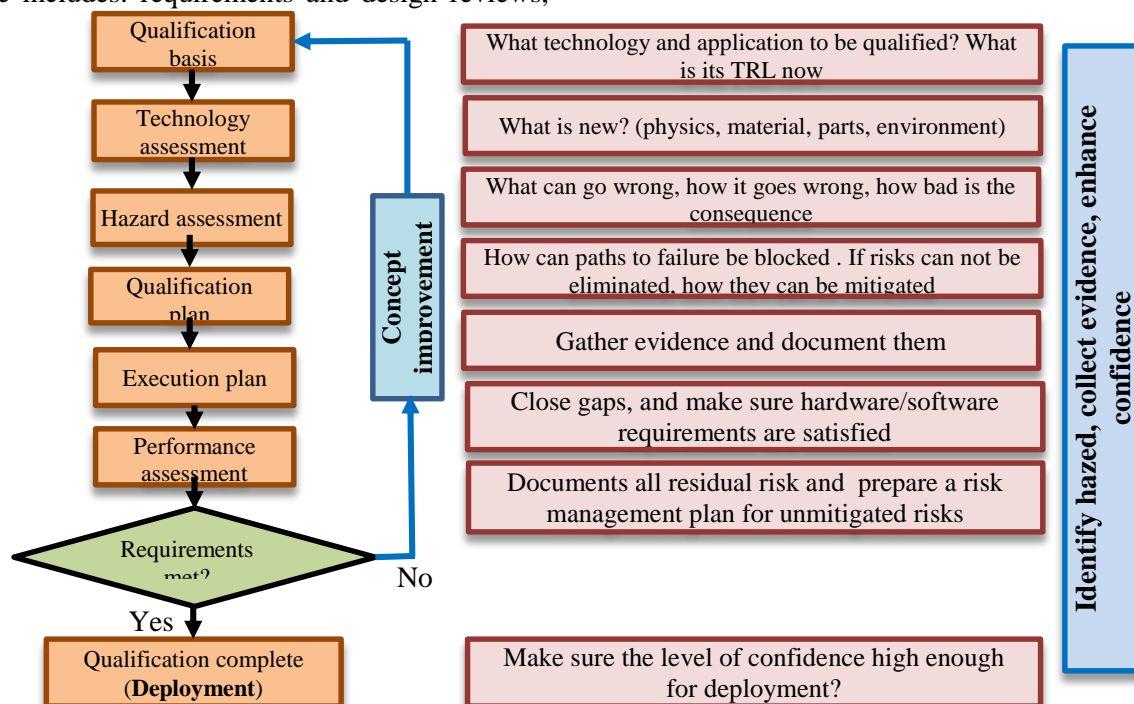

Figure 1: DNV-RP-A203 [8] Technology Qualification Process (TQP).
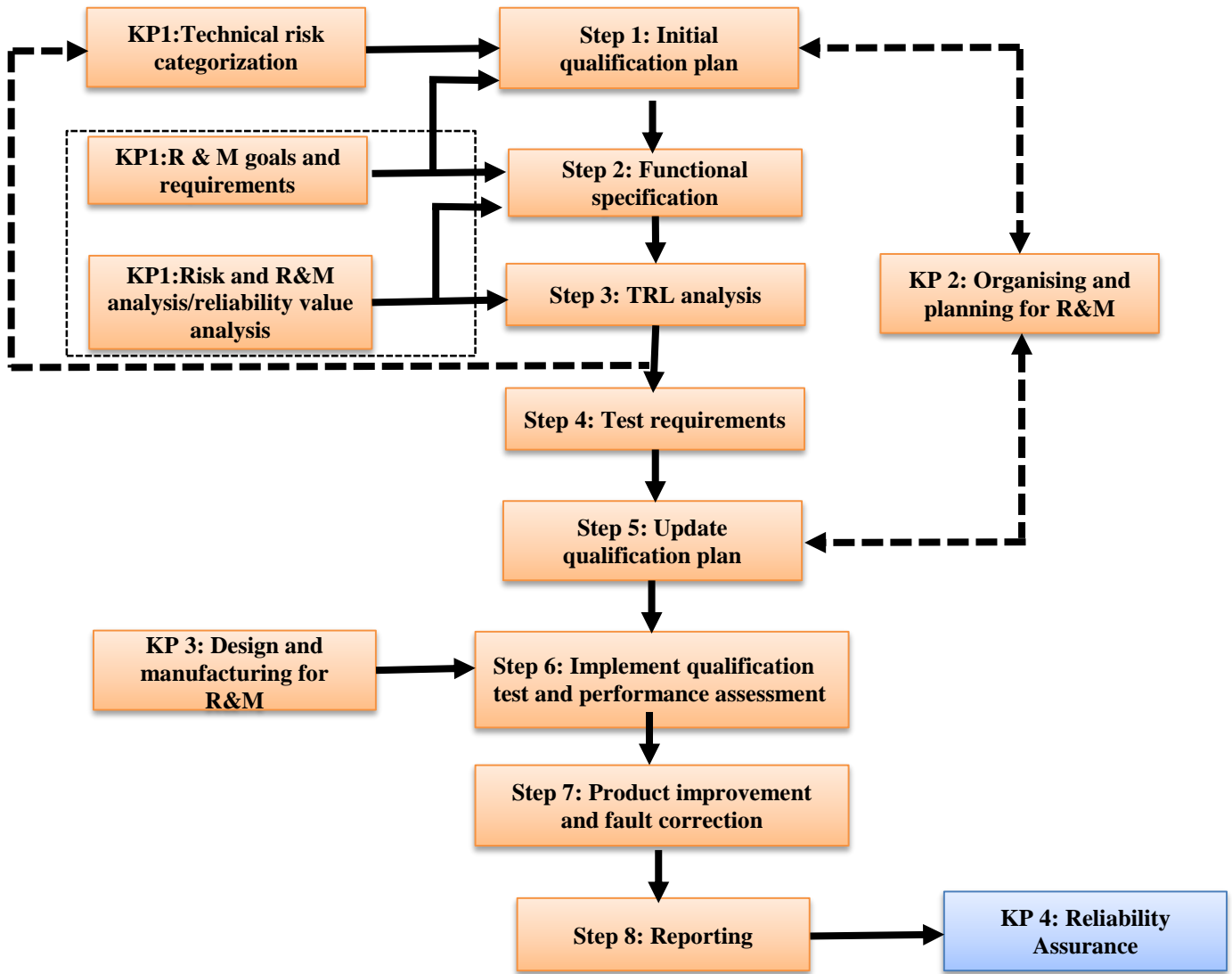
Figure 2: API 17N [3] Technology qualification process

API 17N [3] lists 12 Key Process (KPs) to provide a supportive environment for achieving reliability by managing an appropriate level of reliability throughout the lifecycle of a subsea field (Figure 3).

The philosophy behind codified recommendations is technology may undergo a step change or gradually evolve to meet efficiency, reliability and safety needs. Materials or parts may be different in two pieces of equipment designed by the same manufactures even using the same physical laws. For example, even existing, proven technology may be required to operate in more challenging environments; beyond existing industry experience. When this happens, additional technical risks and performances may be uncertain. One way to manage these risks is through analysis, qualification and testing.

The intent is to provide traceable evidence that systems are qualified through a detailed understanding of service demands, performance requirements and potential failure mechanisms.
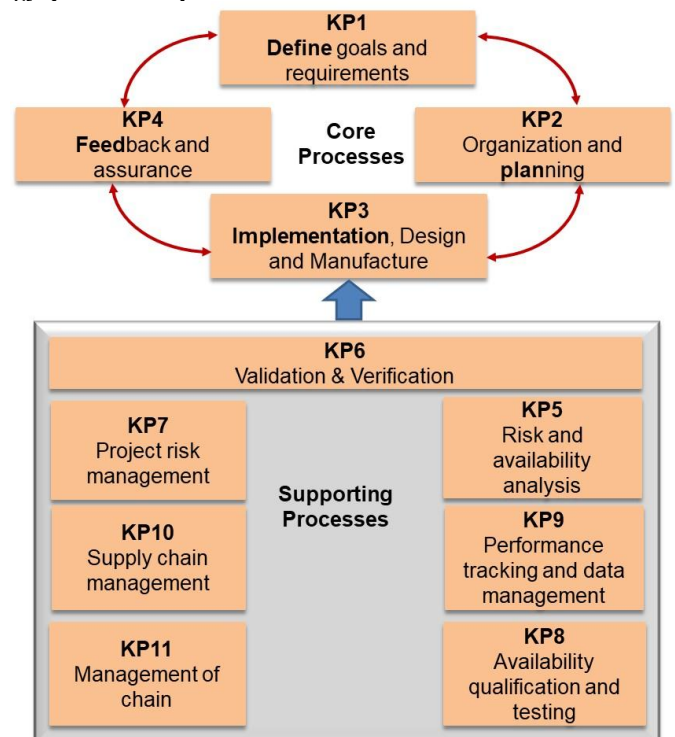

Figure 3: 12 Key Process (KPs) of API 17N and their relationship

According to API RP 17N [3], Reliability Qualification and Testing is a systematic technical risk assessment and risk management approach which includes:
- Definition of technology requirements (includes risk and reliability requirements);
- Identification of technology failure modes and mechanisms;
- Assessment of failure criticality (risk consequences), to determine relevant actions taken to reduce risk and uncertainties;
- Testing to demonstrate functional performance;
- Technology Readiness Level (TRL) to indicate the extent to which an item is "ready for use", given specified qualification factors/requirements;
- Use of test data to estimate reliability.

API RP 17N [3] is a high-level philosophy, while DNV RP A203 [8] is a detailed guidance. The primary focuses of these codes API RP 17N are:
- Focusing on reliability activities such as Reliability Qualification and Testing (KP8);
- Considering operational reliability failures.

Note: Reliability engineering doesn't consider reputation/commercial, safety, and environmental risks.

DNV-RP-A203 [8] defines qualification as "confirmation by examination and provision of evidence that the new technology meets the specified requirements for the intended use." The primary focuses of DNV-RP- A203 [8] are:
- Reliability - this is one of the targets along with performance, safety, environment and other project specific requirements included in the Qualification Basis document;
- Consideration of all types of failures;
- Flexibility to include project specific requirements such as high pressure and high-temperature readiness.

The embed intention of all codes (Hother and Hebert, [16]) are:
- Risk reduction to increase the probability of success;
- Ensuring that the product is "Fit-For-Purpose" before insertion into the system;
- The early part of qualification (FAT and EFAT) are performed by the producer and witnessed by the Client or a third party. SAT and SIT are performed by specialist Contractors appointed by the Client;

- System tests and acceptance tests are performed by the Primary Design Contractor in collaboration with the Client's Operations Team.
- A vendor, who offers a new equipment, is required to provide a proof of fitness for purpose.

According to this definition, qualification means verification& validation.

Systems engineering qualifications (known as verifications and validation (V&V)) are performed by a combination of analytical and numerical methods and testing. At the design stage, mostly analytical methods (FE and CFD) are used, after manufacturing a plethora of tests are used.

The list of methodologies to collect evidence for the reliability assurance is long, and there is some overlap between them. Any procedure is chosen, as well the extent of details is on the 'need' basis and they are situation dependent. The list includes activities which are part of the design and are naturally indispensable. The hypothesis is that the design methods, however exhaustive they are, cannot tease out all probable causes of failure beyond a reasonable probability. Rational choices are required to avoid activities yielding little value. However, at least two different approaches are needed to trap a fault. Any single procedure may be necessary but not sufficient on its own. Analyses and simulation may be used to reduce the number of tests that would be needed to assure the desired system dependability. They can also replace testing when testing would be impossible or expensive.

4. Systems Engineering V-Model

Systems Engineering (SE) is the art and science of developing an operable system capable of meeting the Client's requirements within opposing constraints. SE is a holistic, integrative discipline, wherein the contributions of the Subsea Engineers, Structural Engineers, Electrical Engineers, Mechanical Designers, Power Engineers, Control Engineers, and many more disciplines are evaluated and balanced, to produce a coherent design that is not dominated by the perspective of a single discipline. (see e.g. NASA Systems engineering Handbook [28],). An alternative definition is: Systems Engineering is an iterative process of top-down synthesis, development, and operation of a real-world system that satisfies, in a near optimal manner, the full range of requirements for a system. (INCOSE Systems Engineering Handbook [20])
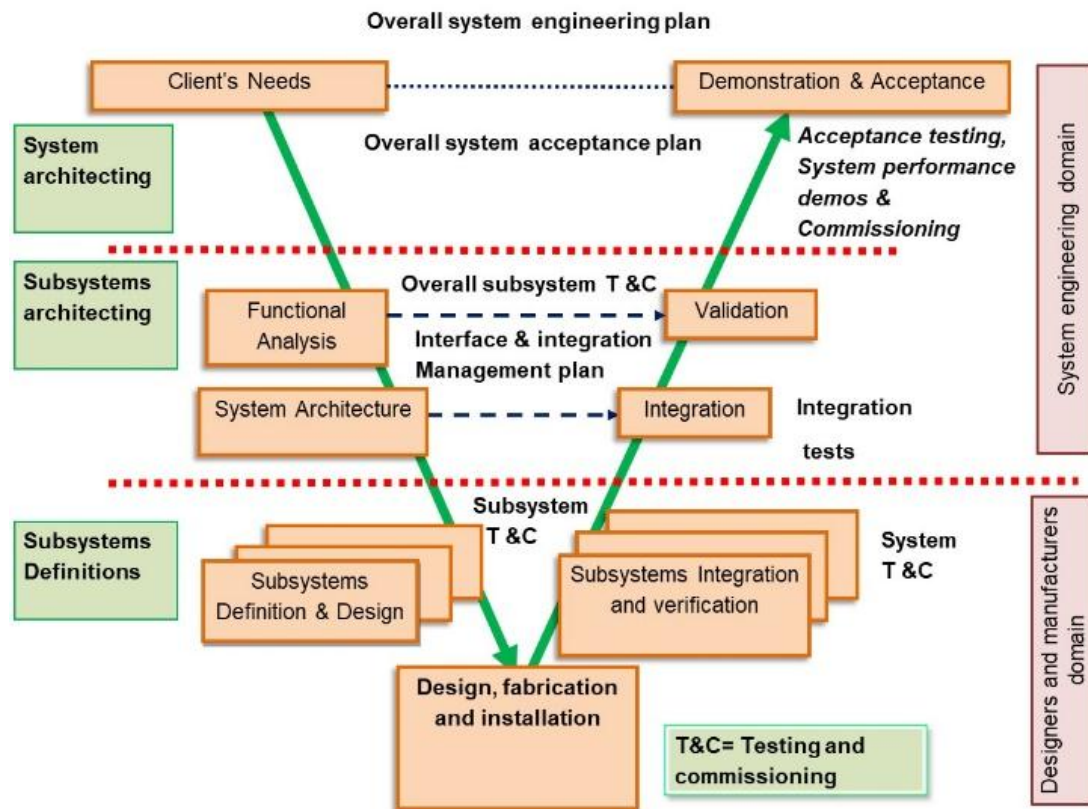
Figure 4: SE V-model for product development

The V-model is one of several models used in SE to visualise the process of a project development. The V-model describes the activities and results that must be produced during development (Figure 4). The left tail of the V represents the *system specification stream*, where the system requirements and the system and subsystem or component designs are specified. The designed components are then fabricated and installed at the bottom of V. Component fabrication is followed by the *testing stream* in the right tail of the V, where the gradually evolving and growing system is verified against the specifications defined in the right tail of the V.

Certain subsystems of the SPS are outsourced to suppliers. These suppliers conduct the complete design, development and testing of the subsystem, and deliver the finished product to the site. Thus, in these cases, the development of the subsystem can be considered as an independent project.

The V-model separates the disciplines of systems and component engineering. This way, *top-down* and *bottom-up* development approaches are integrated into the V-model. That is, the system is specified top-down and then the subsystems are integrated bottom up. Additionally, the definition of distinct steps for the design, at different hierarchy levels, appears first in the V-model and enables breaking down of the system into independent subsystems. The Client's ConOps [20 and 28] are also reviewed, analysed, and transformed into verifiable requirements that define *what* the system will do, not *how* the system will do it, i.e. OpsCon [20 and 28]. Working closely with the

Client Engineers, the requirements are elicited, analysed, validated, documented, and base-lined. The Client's specifications describe what, why and purpose. This ensures that the facility, or equipment, can be used for production as the Client required.
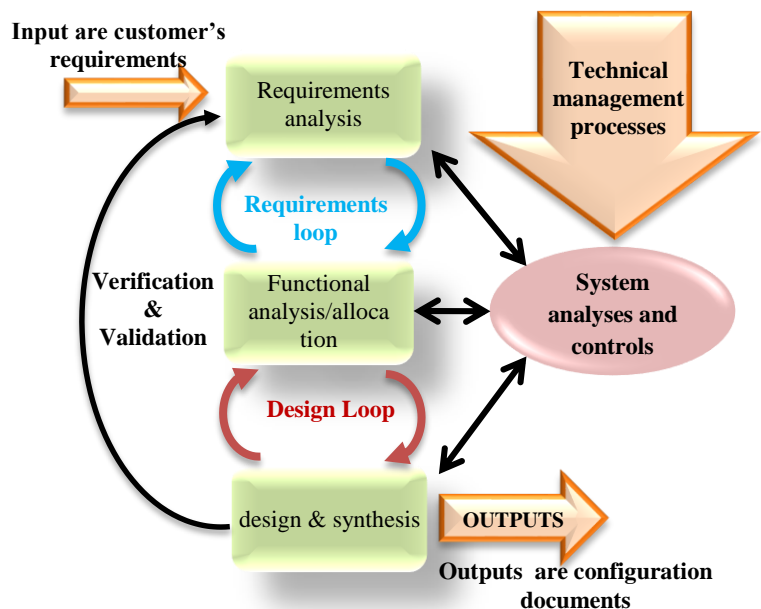

Figure 5: Loops of the development process. See also Figure 6 for details

The system is then decomposed (broken down) into functional subsystems, which are easier to handle. Subsystems can then be designed and fabricated *in parallel*, according to the system specifications defined in the previous phase. When it comes to the

development of highly complex systems, the independent, concurrent development of subsystems is a great way to accelerate the project pace and supports a better involvement of vendors.

Another benefit of the V-model is that it breaks down system definition and V&V into three separate stages (Figure 5). These three main stages, shown in the right tail of the V in Figure 4, form three iteration loops in the development of the system with increasing scope and complexity (Figure 5). The first design loop is at the component or subsystem level. In case of a modular design, the subsystem verification can be performed in parallel, independently of each other. That is the three phases of component design, fabrication, and verification in the bottom of the V consist of numerous parallel Vs, as many as subsystems that are built into the system.

The second loop of system design involves system-level design verification. In this loop, the integrated design is verified against the system specifications delivered in the second Lifecycle Phase in the left tail of the V. Unambiguous and robust subsystem and interface specifications, and a thorough subsystem-level verification facilitates the system-level verification. The third and last design iteration loop in the V-model is the system validation loop, also called system qualification. The outcome of this usually requires a very long, expensive, and comprehensive test procedures that have the objective to prove the developed system satisfies the customer's needs, as well as industry standards and government regulations.

5. Requirement Analysis

Quality only has a meaning in relation to the purpose of the product or service. If something does the job for which it is designed (FFS), then it is a quality product or service.

A subsea project starts when the business case is made during the Appraisal Phase (Yasseri [38]). Technical, economic, and political feasibility is assessed; benefits and costs are estimated, and key risks are identified. In the next phase, known as the Select Phase, alternative concepts which meet the project's purposes and needs are explored, and the best concept is selected and justified using trade-off studies. The project stakeholders reach a shared understanding of the system to be developed and how it will be operated and maintained. The Concept of Operation (ConOps) is documented to provide a foundation for the more detailed analyses that will follow. This will be the basis for the system requirements that are developed in the next step.

Figure 6 shows three loops of a product development with more details. The first loop is the requirements that express the purpose of a system. How well a system fulfils its purpose, or how well it suits its purpose, indicating how good a system is if it is designed in a specific way.

Requirements analysis provides a framework for understanding the purpose of a system and the contexts in which it will be used. It bridges the gap between, an initial vague recognition that there is a need to which subsea engineering can be applied, and the task of building a system to address such a need (Figure 7).
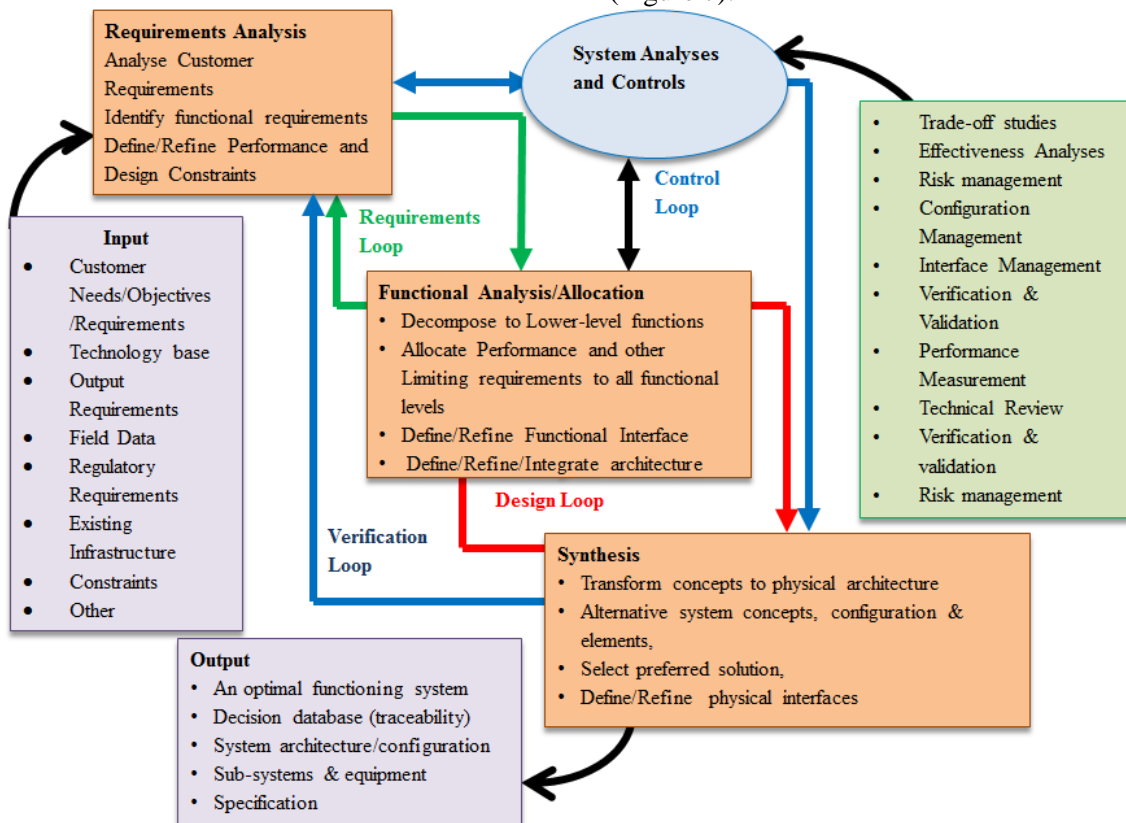

Figure 6: Three loops to reach the implementation stage (adapted from NASA's Handbook [28]). See also Figure 5.
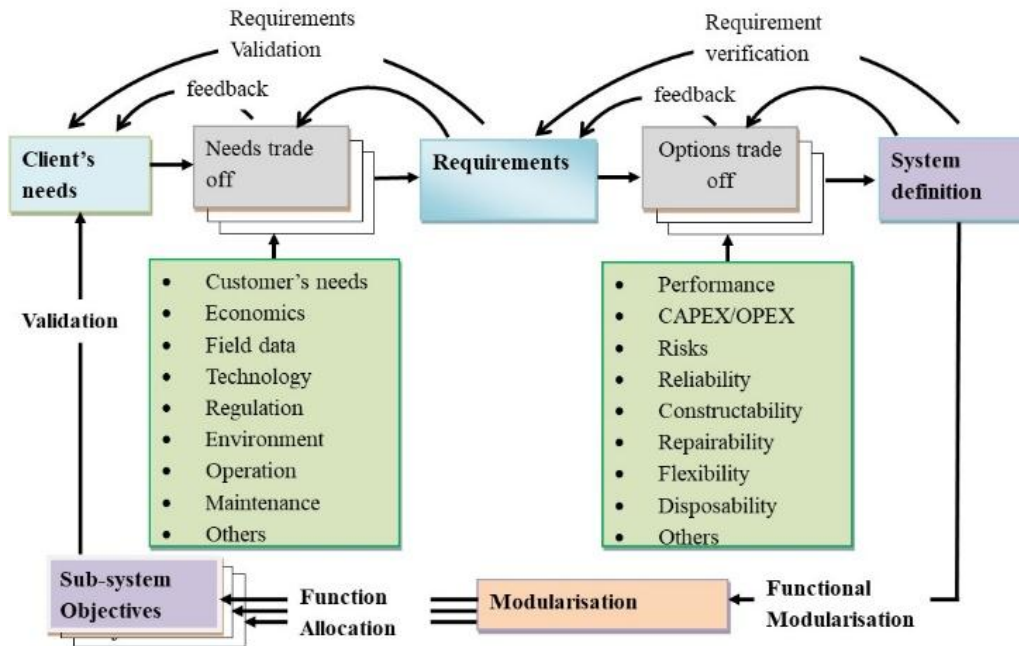
Figure 7: The expanded requirement loop (Figure 5) of Systems engineering process as applied to the subsea development

In seeking to describe the purpose of a system, one needs to look beyond the system itself, and into the activities that it will support. For example, the purpose of a banking system is not to be found in the technology used to build it, but in its day-to-day business activities in fulfilling the needs of its customers. Thus, requirements are a set of activities concerned with identifying and communicating the purpose of a system and the contexts in which it will be used. Requirements act as a bridge between the real-world needs of the Client, and the capabilities and opportunities afforded by technologies.

Requirements engineering is the disciplined and systematic approach to elicit, specify, analyse, commit, validate, and manage requirements while considering user, technical, economic, and business-oriented needs and objectives. It spans the entire lifecycle, often involving distributed teams and supply chains. Understanding the requirements and making sure they are complete and stable are two important aspects of the SE processes, as the rest of the activities are derived from these requirements.

Requirements engineering offers three general principles that are useful in dealing with the complex problems:

• Abstraction: i.e. ignoring the details so that one can see the big picture. The system logical architecture is an abstraction of the system functionality;

• Decomposition: i.e. breaking down a system into parts, so that one can study them independently from each other, and by the different Specialist Engineers. Decomposition in subsea engineering is performed along the line of vendors' specialisation. Such decompositions are never perfect, because of the coupling between the parts, but it offers insights into how things work as well as identifies competent design and manufacturing;

• Projection: i.e. adopting a view or perspective of how the system works, and describing only the aspects that are relevant to that perspective. Unlike decomposition, the perspectives are not intended to be independent in any way (Figure 8).
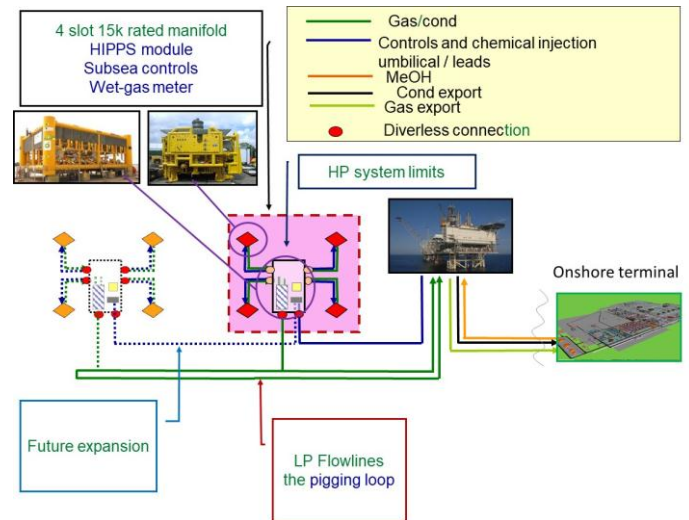

Figure 8: An example of a functional architecture. Physical elements are also sown on the diagram.

Requirement analysts use them to understand what is needed and to identify parts that satisfy the needs of a system. Use of decomposition, abstraction and projection make problems simpler, by mapping existing solutions to problems (or needs). For example, one may look for decompositions in which some of the parts are familiar. In the ideal case, this leads to sub-problems that are sufficiently well known that they have standard solutions. However, one may still have substantial work to do in adapting these known solutions to the new problem context.

A single requirement may have consequences in many parts of a design, program, and data, and may need

many test cases to verify (Federal Aviation Administration, [12]). How a system should interact with its users is also a requirement. There are two types of requirements:

• Functional requirements, which specify what the system should do, i.e., the services the system should provide, and the way it should be provided.

• Non-functional requirements, which specify constraints on how the system should operate and the standards for its operation. Non-functional requirements deal with the characteristics (attributes) of the system that cannot be expressed as functions - such as reliability maintainability, availability of the system, etc.

Non-functional requirements may include:

• Adaptability (expansion);
• Transportability, lift-ability, constructability etc;
• Control-ability such as fast shut down and startup;
• Human-computer interface issues;
• Constraints on the system implementation, etc.

Requirements for a subsystem or a part of the system, do not stem from the technical requirements alone but are only one aspect, of the overall requirement (Figure 9)

A graphical representation of the Requirements Analysis Process as contained in (ISO/IEC 26702 [24] and IEEE 1220-2005 [19]) is shown in Figure 10. The process is quite complex hence requires tailoring to the problem at hand.
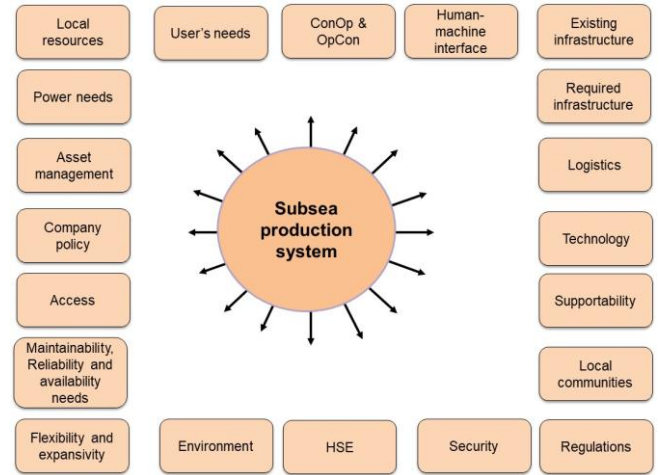

Figure 9: Systems context diagram

6. Requirements Traceability

Requirements traceability will ensure that all higher-level requirements are linked to the lower level requirements, and will be maintained throughout the system development. They are traceable from requirement specifications, through design documents, interface control documents (including operator interface documents) and down to acceptance test procedures. It is important to establish the link

between requirements, supporting design data and information within the design documents, as by providing the original context in which a requirement was selected, any future reconsideration of the requirement can determine if the original constraints are still valid Königs, et al [26]).
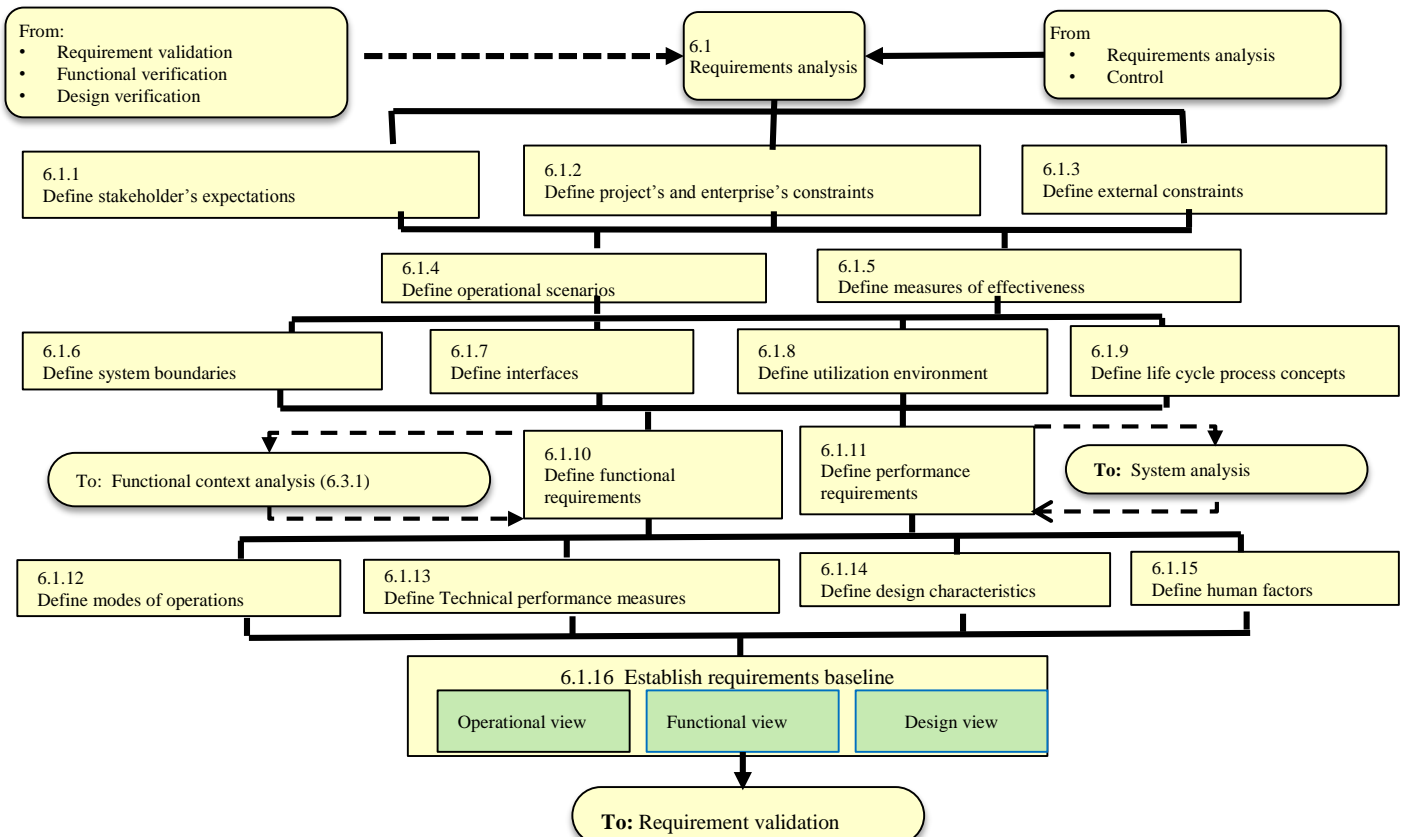

Figure 10: Requirements analysis process of ISO/IEC 26702

Ideally, each requirement from the highest to the lowest level of the project must link to a parent requirement. Requirements without parents will either represent a nice to have or a missing requirement at the higher level. If it is the former, the existence of the requirement must be carefully considered again. In the event of the latter, the requirement needs to be rolled back up to ensure completeness of the requirements at the higher level. A simple trace matrix can be used to simplify and provide a clearer arrangement of the comparison between the user requirements and the technical specifications.

The traceability characteristic means consistent referencing between user requirements, specifications and test cases. This makes it possible to trace cross-references between the specified elements (traceability). To this end, the Client's requirements should be identified with a unique designation, such that referencing is possible.

For each Client Requirement (CR), there must be at least one technical requirement. For each technical requirement (technical specification) there must be at least one specification. The project manager can use the trace matrix in the design qualification to show clearly that all user requirements have been considered. In addition, it can be used to check the completeness of the technical specifications and that the technical implementation corresponds to the requirements. Finally, the trace matrix can be used in the test plan compilation to prove that all user requirements have been tested.

7. Reliability Assessment

Figure 11 shows a subsea project lifecycle. Every Client may have its own lifecycle model, but, they are like what is shown at the top of Figure 11.

A few concepts are developed during the Select Phase and the Conceptual Design. Conceptual Design is an abstract view of the system that shows the only function of all components that make up the system, as well as their inter-relationships. Such diagrams are known as the Functional or the Logical Architecture. One of all the possible Logical Architectures is then selected to be taken forward for the Detail Design Phase. Such choice is based on several criteria, including the lifecycle costs, hence reliability is a major contributor. Modern equipment packages are quite reliable. However, how they are arranged and bundled together will affect the system reliability, as it can affect the Mean Time to Repair (MTTR). Thus, a choice of the architecture based on reliability at the architectural level is the most sensible one.

The Logical Architecture can be improved by performing Reliability and Availability and Maintainability (RAM) analyses, such are MTBF, MTTR and the Reliability Block Diagram (RBD), etc. These methods help to choose the most promising architecture. Generic data (e.g. OREDA [29]) is used to determine the level of availability and how the target availability can be achieved. In the later phase, the generic data is supplemented with the vendor data, and possibly Client database of failures. The Failure Modes, Effects, and Criticality Analysis (FMECA) is
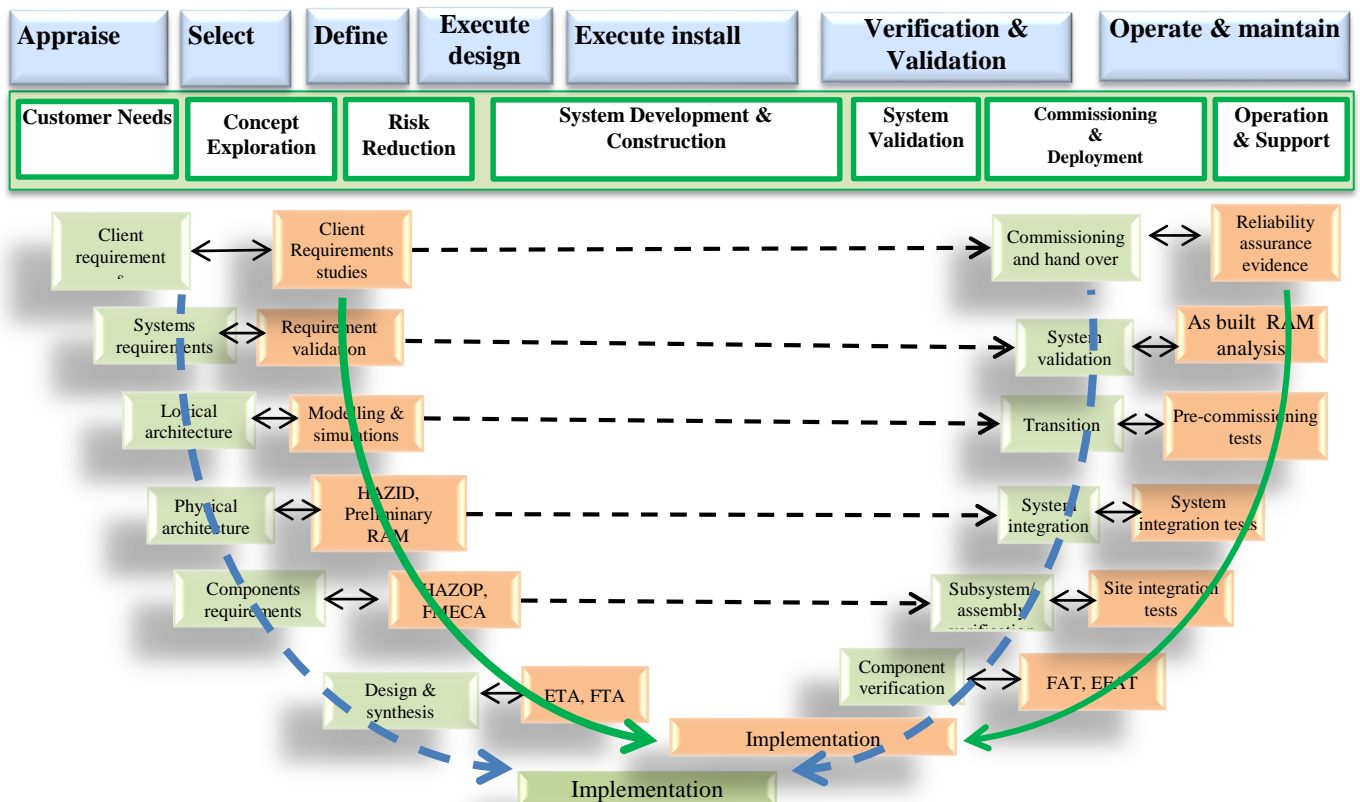

Figure 11: A life cycle model superimposed on the V-model

criticality, rank and suggest corrective and mitigative commonly used to capture all conceivable failure modes and their effects. Usually, FMECA is carried out in the Define Phase and revisited in the Execution Phase (detailed design) of a system, when the physical architecture of the system has taken shape. The objective of an FMECA is to reveal weaknesses and potential failures at an early stage, and based on their modifications to the design. The level of detail and the focus of analysis depends on when the FMECA is carried out. RAM analysis of a system at the early stage of a development can be challenging, especially when system components are not clearly defined. Nonetheless, at early stages of system development, RAM analysis can be used to verify system adherence to target availability requirements. One important step prior to performing a RAM analysis is the need to create a Systems Description Document, which identifies the functions of all the sub-entities of the system and highlights the interfaces between them. In addition, this document also captures the anticipated performance metrics of the system's entities, which are critical inputs for RAM analysis at the conceptual stage of development.

A core activity of reliability assurance is identifying all ways in which the system can fail to perform. This is the case when one or more required functions are disabled (e.g. exceeding the acceptable limits). When this happens, it is called a failure; the resulting state is termed a fault. A fault can be termed as a failure mode. Each function may have several failure modes, and each failure mode may have several different causes, mechanisms and effects (Rausand and Høyland [32]) The failure mode of a component will act as a failure cause of the subsystem, whose resulting failure mode then causes failure of the next level and so on.

In the Define Phase, when no or very few hardware solutions are known, a functional FMECA is done by identifying potential failures for each function according to the hierarchy established in the function tree. In the physical design phase, an FMECA for interfaces is used to verify compliance with the requirements across the interfaces between components and subsystems. In the Define Phase, by selecting vendors, the logical architecture is gradually converted into the physical architecture of the system. At this phase, the specification for hardware and even the candidate vendors are identified and possibly invited to tender. Towards the end of this phase, vendors are selected, and contracts are awarded. The Define Phase is the best time to start reliability analysis of packages.

When hardware and software solutions are decided for the various functions in the Detailed Design (execution) Phase, a System Breakdown Structure showing the hierarchy of components and subsystems is constructed, this is like the Function Trees as shown in Figure 12. With the breakdown structure as input, a detailed FMECA identifies system failures by starting with the failure modes at the lowest level and then proceeding upwards in the hierarchy until the system level is reached.

The FMECA is done by answering a set of questions (Rausand and Høyland [32]):
1. How can each part conceivably fail?
2. What mechanisms might produce these modes of failure?
3. What could the effects be if the failures did occur?
4. Is the failure in the safe or unsafe direction?
5. How is the failure detected?
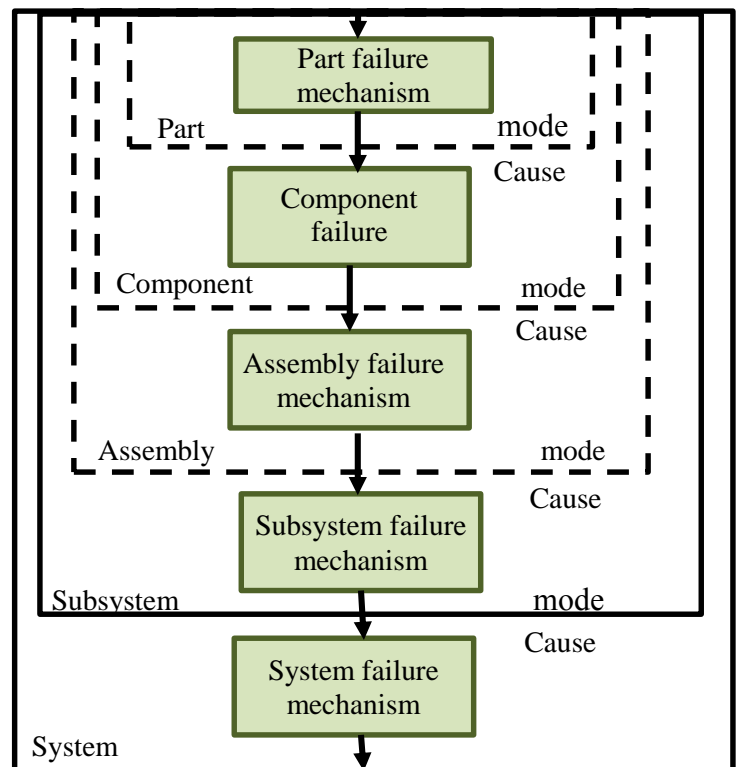6. What provisions are provided in the design to compensate for the failure?

Figure 12: Failure process flow (adapted from IEEE [19])

Another metric used is Technology Readiness Level (TRL) analysis. This is used to track the progress of the system towards the Operational Phase as the system matures (Yasseri [37] and API 17N [3]). TRL (Figure 14) is not an indication of the quality of technology implementation in the design. The TRL analysis, as it stands today, allows any equipment that has been used before to enter the system at TRL 4 or perhaps arguably at TRL 5 (Yasseri [39]). The argument is that a new field is not the same as the existing one, which is true. The consequence of this ranking is everything must be qualified for the environment. This attitude can be explained by considering that in reliability analysis of component/part failure data, the databases used are averaged and generic. Thus, testing only can remove some of the uncertainties.
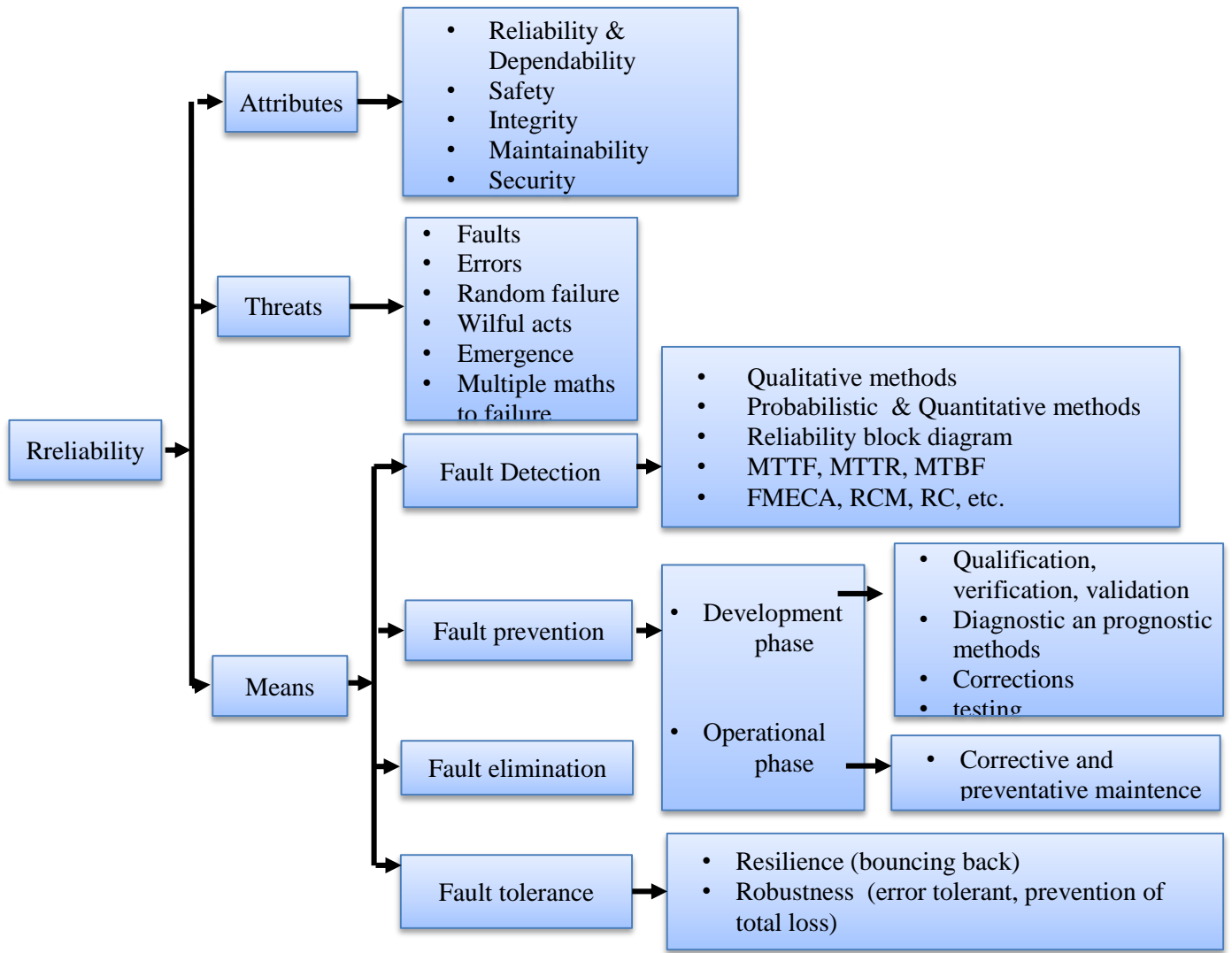
Figure 13: Components of reliability analysis.

Phase	TRL	Development stage completed	Uncertainty reduction
System validation	7	**Field proven** Production system field proven	Maintain qualification of aging system
	6	**System installed** Production system Installed and tested	Commissioning tests
Technology validation	5	**System tested** Production system interface tested	Validation testing , RAM for as the built system
	4	**Environment tested** Preproduction system environment tested	Verification testing
	3	**Prototype tested** System function, performance, and reliability tested	RAM analysis using vendor data
Concept validation	2	**Validated concept** Experimental proof of concept using physical model tests	HAZOP, FMECA, Fault Tree Analysis (FTA), Event Tree Analysis (ETA).
	1	**Demonstrated concept** Proof of concept as desk study or R&D experimentation	What if analysis, Scenario building , Architectural level reliability, availability and maintainability (RAM) analysis using generic data
	0	**Unproven concept** Basic research and development (R&D) in papers	HAZID, Change analysis

Figure 14: API TRL level and reliability assurance activities

RAM analysis provides a way to verify and validate the current system at each TRL level against established operational requirements of the customer. Because simulations represent the ideal future state of the system, it must be understood that the complexities of manufacturing and subsystem integration reduce the availability of the system when deployed. Therefore, to accommodate for the impact of manufacturing on system availability, RAM analysis is used to improve system design beyond the operational availability requirement of the Client, while ensuring that manufacturing, transportation and installation limitations are addressed during the early stages of system development.

The critical part of a technology is a part (or element) which is new, novel, and the system being developed or acquired depends on it to meet its performance requirements within defined cost and schedule. Given that a TRL determination is, in most cases, based on demonstrated performance, the critical technology must be defined at a level that is testable as well. Some authors also state that technologies may be critical from a manufacturing process or material, measurement, or infrastructure perspective, including whether an organization has a workforce with the necessary skills, knowledge, and experience. For example, some organizations will not consider a technology critical if it is having been determined to be mature, has already been used in the field, or does not currently pose a risk to the development. However, when these technology elements are being reapplied to a different program or operational environment, particularly when being used in a novel way, then the definition of criticality applies to them.

All critical technologies must be identified to achieve a comprehensive evaluation of technological risk. While the process to collect evidence for identifying critical technologies can be straightforward, the determination of what constitutes a critical technology is highly subjective, requiring knowledge, experience, and due professional care. Judgements are needed to decide what technology (e.g., hardware, software) is critical, what makes a technology critical, and at what level (e.g., component, subsystem, assembly and system) it is appropriate to test, demonstrate, and validate key functions of that technology or the system.

Although reliability and safety are different issues, tools used in risk reduction are also used to identify the reliability enhancement. HAZOP and HAZID were originally developed for analysing safety; however, they can also be applied to reliability analysis. HAZOP and HAZID studies are systematic methods for examining complex facilities or processes to find actual, or potentially, hazardous procedures and operations so that they may be eliminated or mitigated.

8. Verification, Validation and Qualification

Components are tested at the factory and delivered ready for integration to produce higher-level assemblies or subsystems. These assemblies are also individually verified before being integrated with others to produce yet larger assemblies (for ease of installation) until the complete system has been integrated and verified. The system is installed in the operational environment and transferred from the project development team to the Client team. The transfer also includes supporting equipment, sparing policy, documentation, operator training, and other enabling products that support on-going system operation and maintenance. Acceptance tests are conducted to confirm that the system performs as the Client required in the operational environment. A transition period and warranty see the transition to a full system operation. The above processes are known as "Verification" and "Validation", which is primarily performed through testing at various stages.

Verification and validation (V&V) are the methods that are used for confirming that a product, service, or system meets its respective specifications and is Fit-For-Service in general terms, verification is a *quality control* process that is used to evaluate whether a product, service, or system complies with regulations, specifications or conditions imposed at the start of the Development Phase (Babuska and Oden [5]). Validation, on the other hand, is a *quality assurance* process of establishing evidence that provides a high degree of assurance that a product, service, or system fulfils the Client's requirements (Plant and Gamble, [31]). Verification and validation have been defined in various ways that do not necessarily comply with standard definitions. For instance, journal articles and textbooks use the terms ''verification'' and ''validation'' interchangeably (e.g. Jagdev et al [14], or Dzida, Freitag [10]), or in some cases there is reference to ''Verification, Validation, and Testing (VV&T)'' as if it were a single concept (Engel [11]) with no discernible distinction among the three terms (Allen et al [1]). The definitions which are given by ISO 9000 [21] originate from the general field of quality and focus on the provision of ''objective evidence'' that specified requirements have been fulfilled. The verification process according to ISO is broadly defined, and validation is focused on demonstrating an intended use or application of a system.

A possible structure for V&V program is shown in Figure 15, which starts with reliability analyses and ends in verification and validation by testing, numerical analyses and simulation; or prototyping. The agreed Client's needs are used to define the requirements, which must be validated to assure if they are achievable, relevant and complete.
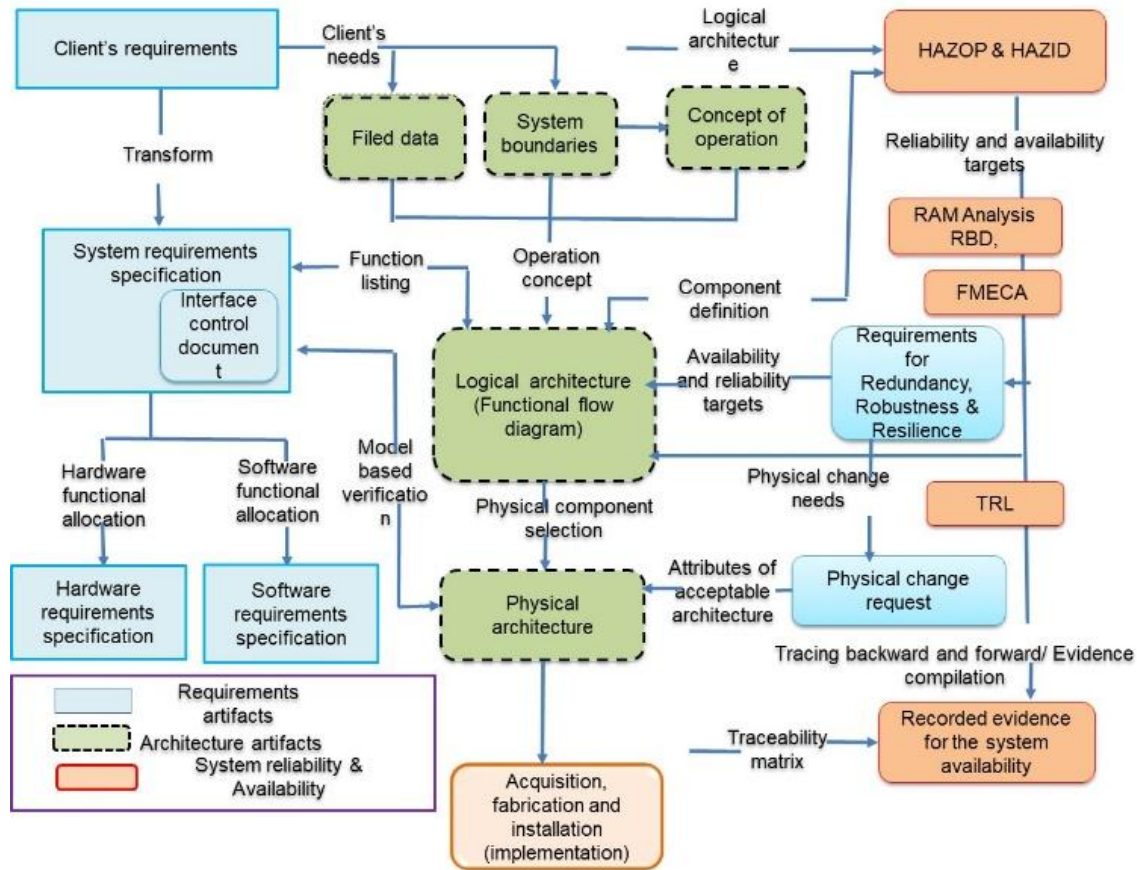
Figure 15: A possible verification and validation flow chart

Tools are qualified whereas processes that use the tools are validated. In this definition qualification is a subset of validation. Fasteners (nuts & bolts) and welding are used to join parts of a system; thus, they are just tools to connect pieces together, but one must also answer if they are Fit-For-Service. In this case:

- One should qualify nuts & bolts or welding material and procedures as a tool for building a system. Perform basic verifications to ensure they are Fit-For-Service;

- One should validate nuts & bolts or welding in assembled equipment for their ability to reliably enable an equipment to deliver the functionality expected of them, presenting evidence from the fasteners qualification tests...

Fasteners are used as an example of a building block. The entire equipment may also be considered as a building block. Such equipment is then qualified using appropriate tests and/or analysis, but a system that uses this equipment needs validation. Thus, qualification tends to be smaller in scope than validation and less dynamic (i.e. qualified for a purpose at a point in time). Thus, according to this definition, qualification is a subset of much greater validation initiative.

Another term often used by some industries is certification. Sometimes certification is used to mean that the performance of the finished product is witnessed by a third party during a specific test, and that party has awarded a certificate of performance;

generally, in compliance with a standard. This usage of the term generally refers to mass-produced items, or items produced based on a specification, when required. The current certification practice is "standards-based", which requires that the prescribed certification process of a standard is followed, depending on the application. For example, IEC 61508[15] is used in industrial applications, ISO 26262 [22] is for the automotive area, whereas DO-178B/C [9] refers to software for airborne systems.

In the pharmaceutical industry, *Validation* is used to mean a systematic approach to collecting and analysing sufficient data to give reasonable assurance and documented evidence that a process or an analytical method will, when operated within specified parameters, produce consistent results (mostly drugs) within predetermined specifications (WHO [36]). When this approach is related to a machine or a piece of equipment, rather than the entire system, then it is referred to as *Qualification*. Qualification is part of, but not limited to, a validation process, which in turn is divided into Installation Qualification (IQ), Operation Qualification (OQ), and Performance Qualification (PQ). In performing these activities, many documents describing plans and approaches to analysis are generated. These include Validation Master Plan, Qualification Master Plan, Risk Analysis, Validation Protocol, Test Protocol (including specification), Validation Report, and

finally a Summary of Deviations/Issues (Melero et al [27], and Todde et al. [33]).

Both the pharmaceutical and subsea industries use the term *commissioning* to mean a methodical and documented process to ensure that as built facilities, systems, and equipment meet design codes and the Client's requirements. It applies to all aspects of a facility, equipment, and services. The commissioning process verifies that what was specified, has been installed; that it functions properly; and that it was successfully witnessed by the Client's Operations Team. It is the last system testing before hand over. Commissioning is a managed and planned process of bringing a facility or equipment from its installed or constructed state into service. The key activities are similar regardless of whether commissioning is applied to the entire facility or a simple piece of equipment. The pharmaceutical industry makes a distinction between commissioning and qualification, where the former is concerned with good engineering practice, and the latter primarily verifies the facility and systems aspects that can affect product quality. In the subsea industry, the systems do not affect the quality of the product.

Adding to the confusion caused by these terms, with similar and overlapping meanings, different organizations mix these terms and definitions further.

9. Verification and Validation Strategy

The V&V strategy consists of a set of actions, each one of which is a kind of trial, test or inspection. There may be several actions defined against each requirement.

Each action should consider the following aspects:
• The kind of action that would be appropriate for the requirement;
• The stage at which each action could take place – the earlier the better;
• Any special equipment that would be needed for the action;
• What would constitute a successful outcome.

Qualification and V & V are sometimes used to mean the same thing in the literature, for example, IEC 60300-3-15 (2009) consider the qualification process to embrace both verification and validation. In his paper qualification and verification are used interchangeably.

Figure 11 shows the V&V strategy along with a time-line above the V-model. The early V&V process relates to the left-hand side of the V-model and later ones to the test stages on the right-hand side. A single requirement will typically give rise to a multitude of verification activities at various stages of the development. Where a requirement is satisfied through useful emergent properties, qualification of components alone is insufficient; tests must be carried out at the level where emergent properties manifest themselves.

The V&V actions should be commensurate with the level of requirements in the hierarchy. For example, Client requirements give rise to commissioning trials, whereas system requirements give rise to system tests, that is, prior to hand over to the Client. It is not necessary to define system tests against Client requirements since systems requirements are derived from the Client's requirement.

This paper sees the test as a tool (while V&V are Processes) to provide evidence alongside other tools such as simulation and analyses using suitable models, codes compliance checks, inspection and reviews. These tools must be qualified to ensure they deliver what is demanded of them.

Purely test-based V&V or purely analytical-based V&V can lead to some faults remaining undetected. A balanced use of both has the greatest chance of reducing the cost and enhancing the confidence. From a V&V perspective, the assurance evidence is collected throughout the development lifecycle in the form of formal analysis of the architecture and design. Testing is used to fill the gaps as analytical models cannot detect fabrication errors, or visual inspections cannot be used to accept defects.

Typical steps in the verification and validation process are as follows:

Step 1. Identify Test Needs. Requirements and specifications are used to determine what tests must be carried out. This step also serves to establish how the requirements will be validated. For manufacturers of electro-mechanical products, given their multiple functional domains, this step will serve to identify testing required for mechanical, electrical, and embedded software, as well as for the combined system.

Step 2. Secure Test Facilities and Resources. This entails securing the facilities for building physical prototypes, and then executing tests and/or assigning resources to develop models and run simulations

Step 3. Prepare Test Cases and Test Configuration. Design requirements are translated into a set of test cases with procedures and constraints that can be digitally and/or physically measured. Additionally, new test configurations (which may be mechanical, electrical, and/or software-based) are developed considering the current design (e.g. modifications to geometry, materials, and substituted components). Then, the fixtures and rigs are designed to support testing.

Step 4. Setup and Execute Test. This step calls for the setup and execution of the digital simulation models or the physical tests across all functional domains.

Step 5. Document and Deliver Results. Lastly, results of the physical and/or digital tests are documented in reports, demonstrating that requirements and specifications have been met. The correlation between

simulation and physical tests is documented. Results are then delivered to the submitter to identify passed/failed requirements and recommendations for failures that were encountered.

10. Evidence Gathering

Two sub-processes are used to derive the V&V strategy, i.e. acceptance criteria and quality strategy.

The answer to the question 'what will convince the Client that all requirements have been satisfied?', can often lead to a clearer and more focused formulation of requirements. This question can be answered in two ways:

• The Client may define an operational situation in which the requirement can be demonstrated, and/or,
• The Client may define a numerical value for a level of achievement that must be demonstrated.

The first type of answer feeds directly into the process of creating a set of tests, trials or demonstrations that must be part of the V&V strategy. The second type of answer indicates the 'pass mark' for a trial test or demonstration, i.e. it indicates the acceptance criterion for the requirement. Acceptance criteria define, for each requirement, what would be a successful outcome from the qualification approach adopted.

For one-off systems such as SPS, it is necessary to make sure that all the functionality has been properly provided and that the production personnel are happy that the system can be used easily and quickly on demand. This will require a mixture of tests and trials. First, the capability of the system under test loading must be demonstrated. If this capability is not acceptable, then there is no point in progressing to tests that involve much more investment such as live trials at full capacity.

The Client's needs are used to set the initial requirements and are frequently referred to as part of the validation activity. Initial model validation is done

to ensure that the models, analysis and simulations can be used safely to support requirements validation. In addition to performance analysis, modelling and simulation, requirements validation can include risk analysis, such as Fault Tree Analyses and Probabilistic Risk Analyses, to ensure the design will be robust against failures or system upsets (IAEA-TECDOC-1264 [15]).

Flow assurance analyses are performed to study the limits of operation as well as for production planning. This helps with studying the sensitivity of the operational needs to changes in key reservoir parameters. Monte Carlo simulation is another useful tool for assessing the robustness of a system in terms of its overall performance; especially during a system upset.

11. Discussion

The key concepts to establish linkages between requirements and testing for Validation & Verification are shown in Figure 16. At each level of the system decomposition, requirements are flowed-down and suitable test plans are devised for verifying that the system will satisfy requirements. To make sure all requirements are properly implemented, it must be possible to trace each requirement to a component and vice versa. Requirements traceability is the ability to link every requirement to three related items:

• The Client's needs (the starting point) that it fulfils;
• The system elements implemented to satisfy it;
• The test case that verifies it.

The end-to-end traceability links enable us to evaluate exactly what is impacted by the latest requirement change, or an alternative design choice before the change is implemented.
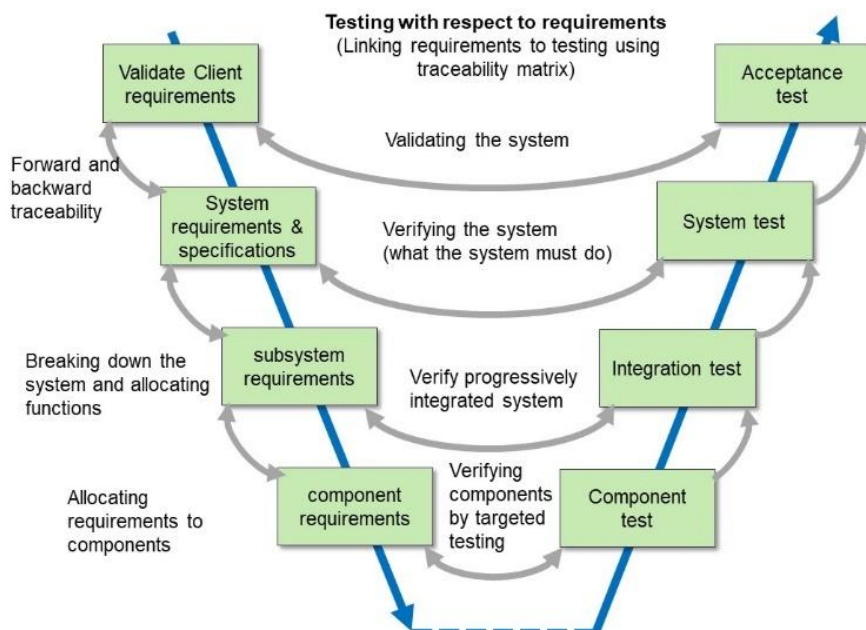

Figure 16: Linking V&V to the Client's requirements

FAT (Factory Acceptance Tests) and EFAT (Extended Factory Acceptance Tests) performed on components are documented to use in a traceability matrix. This ties the tests back to the specific requirements they verify and ensures that no requirement is left untested. Hardware and software components, which are already verified by tests, are then integrated into modules or subsystems and tested. The goal at this stage of testing is to ensure that all the interfaces between components and assemblies are satisfactory and that all subsystem requirements and constraints have been considered. An integration plan is devised that defines the order in which lower-level components and subassemblies are integrated. At each integration step, the functionality of the sub-assemblies against the appropriate set of requirements is verified using the Subsystem Verification Plan devised during the Design Phase. Tests performed to verify requirements at the component level are important since many requirements are cascaded through multiple levels of system decomposition.

The goal of system acceptance testing is to validate that the system fulfils its intended purpose. During the Conceptual Phase, key Client needs, overall system capabilities, usage scenarios (CONOPS and use cases) and performance measures for system validations are identified. A *System Validation Plan* is devised and monitored using change control, which ensures that the verification plan, or test procedure, is not wrong or out-dated. When verification testing indicates a problem, the requirements and design must be reviewed to see what, if any, adjustments are necessary (Bahill and Henderson [6]).

Pieces developed independently don't always work when integrated together, which is arguably the largest single factor that causes schedule and cost overruns. Thus, the Systems Engineers have devised the following policy to minimize this risk:

- Verify interfaces and interactions between key subsystems and components early by use of models and simulations;
- Integrate parts progressively.

12. Concluding Remark

Qualification is used, in this paper, to mean 'a state of readiness to operate', which must be maintained as the equipment ages. The term qualification is also used to mean that materials, design, fabrication and performance under intended use, are verified by a combination of analyses, simulations and testing, throughout the project life. Traditional *quality control* assures that the product will work after assembly and as designed. Whereas *reliability* provides a probabilistic assurance that an item will perform its intended function for a defined period without failure under specified conditions. In other words, reliability looks at *how long* the product will work as designed, which is a very different objective than that of traditional quality

control. Therefore, different tools and models apply to reliability, do not necessarily apply to quality and vice versa.

The focus is on the continued function and resilience of critical assets to prevent interruption of functions. Reliability assurance is a common integrative framework, not a single policy, to design in robustness and resilience and to reduce breakdown due to mechanical failure, accidental event and willful actions. Reliability assurance also relies on existing protection and mitigative policies, including material selection, corrosion protection, accident prevention external hazards, geotechnical hazards etc. The effectiveness of reliability assurance should be measured in relation to availability and continued operation. The present framework merges with the wider issue of risk management framework and the strategic objective of the owner.

The verification strategy is defined as combining efficiently the different verification stages, verification levels and verification methods, to reach the following objectives:
- Satisfy the Client's requirements;
- Maintain cost targets;
- Respect schedule constraints.

The initial step of the verification process is the identification of the requirements to be verified. The general requirements are analysed to originate system and lower level specifications containing a consistent tree of performance addressing; design, interface, environmental, operational and support requirements, which form the basis of the verification activities at the different levels. To facilitate the verification implementation in terms of planning, execution, control and reporting, the requirement generation and allocation activity will ensure specific requirement characteristics; each requirement shall be:
- *Traceable* with respect to one or higher-level requirement;
- *Unique* and associated with a proper identifier (document and paragraph number);
- *Single* and not containing more than one requirement;
- *Verifiable* with one or more approved verification method;
- *Unambiguous* and containing a precise statement;
- *Properly referenced* to other requirements, with the applicable document and paragraph identification.

In addition to performance analysis, modelling and simulation, validation include reliability analysis to ensure that the design will be robust for all specified operating and environmental conditions, which should also consider all possible deviations from the normal operating condition.

One of the fundamental principles of the subsea industry is that quality must be designed into equipment and processes from the beginning. Facilities and systems must support the quality

requirements of their associated processes to be deemed "Fit-For-Service". Reliability analysis methods help to identify critical aspects of the design to focus on, thus moderating the amount of testing. The term 'critical aspect' is used to mean mitigation control implemented by design, not by procedural controls. Critical aspects can be identified during a risk assessment. Industry uses a plethora of methods for risk identification. HAZOP, HAZID and FMECA are three examples of hazard assessment methods which perform well in the identification of risks.

It was also emphasised the importance of tracing the requirements to their solutions (design), the Requirements Traceability Matrix (RTM) documents show how the analysis of requirements translates into the project-specific design, from which technical specifications can be developed and used to design testing and acceptance criteria.

The subsea industry never intentionally creates requirements and designs that result in operation at the "limit". While a system may be designed to meet performance specifications within a generous set of tolerances, it should be rare to fail rapidly in the event of relatively minor excursions from normal operation. The concept of graceful degradation, without failure, is the key to successfully implementing subsea systems in deeper environments at a reasonable cost and within a reasonable timescale. A properly executed validation program will enable slow degradation by using performance sensitivity analyses and design risk analyses, thus providing the project insight to guide risk versus cost (mitigating action) trades.

13. REFERENCES

1. Allen N.A., Shaffer C.A., Watson L.T. (2005). "Building Modelling Tools That Support Verification Validation, and Testing for the Domain Expert," Proceedings of the 2005 Winter Simulation Conference, Orlando, FL, pp 419–426.

2. ABS, (2017). Guidance notes on Qualifying New Technologies, American Bureau of Shipping, PP 45

3. API 17N, (2014). *Recommended Practise for Subsea Production System Reliability, Technical Risk & Integrity Management*

4. API 17Q, (2010). *Subsea equipment qualification – standardized process for documentation*

5. Babuska I, and Oden JT (2004). "Verification and Validation," Computational Engineering and Science: Basic Concepts. Computer Methods in Applied Mechanics and Engineering 193(36–38):4057–4066.

6. Bahill, A.T., and Henderson, S.J. (2005) Requirements Development, Verification, and Validation Exhibited in Famous Failures Systems Engineering, Vol. 8, No. 1.

7. Bureau Veritas, (2010). *Risk bases Qualification of New Technology Methodological Guidance, Guidance Note NI 5252 R00E*, pp 20.

8. DNV-RP-A203 (2011). *Qualification of new technology*. Det Norske Veritas, Høvik, Norway.

9. DO-178C, (2011), Software Considerations in Airborne Systems and Equipment Certification, FAA

10. Dzida W, Freitag R (1998) Making Use of Scenarios for Validating Analysis and Design. IEEE Transactions on Software Engineering 24(12):1182–1196.

11. Engel, A. (2010). Verification, Validation, and Testing of Engineered Systems. Wiley.

12. Federal Aviation Administration. *Requirements Engineering Management Handbook DOT/FAA/AR-08/32*, 2008, last accessed 23/12/2017, available on. http://www.faa.gov/aircraft/air_cert/design_approvals/air_software/media/AR-08-32.pdf

13. Feiler, P.H., Goodenough, J.B, Gurfinkel, A., Weinstock, Ch. B., and Wrage, L. (2012), SPECIAL REPORT CMU/SEI-2012-SR-013, Reliability Validation and Improvement Framework Carnegie Mellon University

14. Jagdev H.S, Browne, J, Jordan, P. (1995), Verification and Validation Issues in Manufacturing Models. Computers in Industry 25(3):331–353

15. IAEA-TECDOC-1264, (2001), Reliability assurance programme guidebook for advanced light water reactors.

16. Hother, J.A., and Brian J. Hebert, B.J., (2005), Risk Minimization using Failure Mode Analysis in the Qualification of New Technology - Recent Project, SPE-96335-MS, SPE Annual Technical Conference and Exhibition, 9-12 October, Dallas, Texas Experience

17. Hull, E., Jackson, K., and Dick, J. (2002). *Requirements Engineering*, Springer-Verlag, London.

18. IEC 61508, SC 65A, (2010), Functional safety of electrical/electronic/programmable electronic safety-related systems in seven parts.

19. IEEE 1220-2005, 2005, reaffirmed in 2011, Standard for Application and Management of the Systems Engineering Process

20. INCOSE 2015. Systems Engineering Handbook – A Guide for System Life Cycle Processes and Activities, version 4.0. Hoboken, NJ, USA: John Wiley and Sons, Inc., ISBN: 978-1-118-99940-0.

21. ISO 9000 (2005) *Quality Management Systems: Fundamentals and Vocabulary*, ISO organisation

22. ISO 26262 (2014), Functional Safety Standard.

23. ISO/IEC 15288, 2008, Systems Engineering-System Life Cycle Processes

24. ISO/IEC 26702 IEEE Std 1220-2005 First edition 2007-07-15 - ISO/IEC Standard for Systems Engineering - Application and Management of the Systems Engineering Process

25. Lloyds Register, (2017). *Guidance Notes for Technology Qualification*, Published by Lloyd's Register group ltd, London, pp43.

26. Königs, S.F., Beier, G., Figge, A., and Stark, R. (2012). "Traceability in Systems Engineering –

Review of industrial practices, state-of-the-art technologies and new research solutions," Elsevier Advanced Engineering Informatics, 26(4), pp 924-940.

27. Melero, L.T.U.H, da S. Silva K.S., Zanette, C., de Araújo E.B., and Mengatti, J., (2011), Calibration and Qualification of equipment in the Pharmaceutical industry, International Nuclear Atlantic Conference, INAC 2011 Belo Horizonte, MG, Brazil, pp 8, https://www.ipen.br/biblioteca/2011/inac/17018

28. NASA, (2007). *Systems Engineering Handbook*. NASA Technical Report NASA/SP-2007-6105 Rev1, ISBN 978-0-16-079747-7, Washington, DC, USA.

29. OREDA (2009). Offshore Reliability Data. Det Norske Veritas, Høvik, Norway, 5th edition.

30. Pecht, M. (1993). "Design for qualification," Annual Reliability and Maintainability Symposium

31. Plant R, Gamble R (2003) Methodologies for the Development of Knowledge-based Systems. Knowledge Engineering Review 18(1):47–81.

32. Rausand, M. and Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications*, PP 664.

33. Todde,S., Peitl, P.K., Elsinga, P., Koziorowski, J., Ferrari, V., Ocak, E.M., O. Hjelstuen, O., Patt,M., Mindt,T.L. and Behe, M., (2017) Guidance on validation and qualification of processes and operations involving radiopharmaceuticals, EJNMMI Radiopharmacy and Chemistry, 2:8 https://ejnmmipharmchem.springeropen.com/track/pdf/10.1186/s41181-017-0025-9?site=ejnmmipharmchem.springeropen.com

34. Viola, N., Corpino, S., Fioriti, M. and Stesina, F., (2012). Functional Analysis in Systems Engineering: Methodology and Applications, Systems Engineering - Practice and Theory, Boris Cogan (Ed.), ISBN: 978-953-51-0322-6, In Tech, last accessed 23/12/2017, Available from http://www.intechopen.com/books/systemsengineering-practice-and-theory/functional-analysis-in-systems-engineering-methodology-and-application

35. Woody, C., Ellison, R. and Nichols, W., (2014), Quality and Reliability Measures, CMU/SEI-2014-TN-026, Carnegie Mellon University, http://www.sei.cmu.edu

36. WHO- (2016) World Health Organization, Annex 4, "Supplementary guidelines on good manufacturing practice: validation". HTTP:// www.who.int/medicines/areas/quality_safety/quality_assurance/validation-without_appendices_2016_05_17. pdf?ua=1. Accessed 23/12/ 2017.

37. Yasseri S. (2013). "Subsea system readiness level assessment" Int. Journal of Underwater Technology 31: 77–92

38. Yasseri S., (2014). "Application of system engineering to subsea development," Int. Journal of Underwater Technology,32:93–109

39. Yasseri S., 2014, "A measure of subsea readiness level development," Int. Journal of Underwater Technology 32:93–109

40. Yasseri S. (2015). "Evidence-based subsea engineering," Int. Journal of Underwater Technology Vol. 32, No. 2, pp. 93–109,

41. Yasseri S. Bahai, H and Yasseri, R., (2018). "A Systems Engineering Framework for Delivering Reliable Subsea Equipment, 2018-TPC-035, ISOPE 2018, Japan. Accepted for publication

42. Youngblood, S. M., and Pace, D. K., (1995), "An Overview of Model and Simulation Verification, Validation, and Accreditation," *Johns Hopkins APL Tech. Dig.* **16**(2), 197–206.

Abbreviations

Abbreviation	Description
CAPEX	Capital expenditure
CAD	Computer-Aided Design
CFD	Computational Fluid Dynamics
ConOps	Concept of Operations
CR	Client Requirement
EFAT	Extended Factory Acceptance Test
FE	Finite Element
FAT	Factory Acceptance Test
FFP	Fit-For-Purpose
FFS	FitFor-Service
FMECA	Failure Mode Effect Critically Analysis
HAZID	Hazard Identification
HAZOP	Hazard of Operation
KP	Key Process
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
MTBF	Mean Time Between Failures
OPsCon	Operations Concept (OpsCon).
OPEX	Operating expenditure
RAM	Reliability, Availability and Maintainability
RTM	Requirements Traceability Matrix
SAT	Site Acceptance Test
ROV	Remotely Operated Vehicle
SPS	Subsea Production System
TRL	Technology Readiness Level
V&V	Verification & validation
VV&T	Validation, Verification & Testing