DNV

RECOMMENDED PRACTICE

DNV-RP-A204

Edition October 2020
Amended September 2021

Qualification and assurance of digital twins

Preview copy

[Only the chapters in full color shown in the chapter overview are available in this document]

DNV AS

FOREWORD

DNV recommended practices contain sound engineering practice and guidance.

Any comments may be sent by e-mail to *rules@dnv.com*

CHANGES – CURRENT

This was a new edition in October 2020 and has been amended latest in September 2021.

The numbering and/or title of items containing changes is highlighted in red.

Amendments September 2021

Topic	*Reference*	*Description*
Rebranding to DNV	All	This document has been revised due to the rebranding of DNV GL to DNV. The following have been updated: the company name, material and certificate designations, and references to other documents in the DNV portfolio. Some of the documents referred to may not yet have been rebranded. If so, please see the relevant DNV GL document. No technical content has been changed.

Editorial corrections

In addition to the above stated changes, editorial corrections may have been made.

Acknowledgements

This recommended practice has been initiated and developed in close collaboration with TechnipFMC. The methodology has been tested and enhanced based on discussions with Aker BP. Both organizations are acknowledged for their contributions.

CONTENTS

SECTION 1 GENERAL

1.1 Introduction

Digital twins mirroring assets are increasingly being applied in industry. Digital twins will impact decisions from early design to decommissioning, hence it is paramount to ensure confidence that the digital twin will function as specified and that the information can be trusted. Lack of trust will limit the value provided by the digital twin.

DNV has responded to this challenge by establishing a recommended practice for the qualification and assurance of digital twins. The methodology is based on DNV's experience with technology qualification (DNV-RP-A203), assurance of data quality (DNV-RP-0497), and assurance of simulation and data-driven models (DNV-RP-0510 and DNV-RP-0513).

1.2 Objective

The objective of this document is to describe a structured and systematic process and set requirements for the qualification and assurance of digital twins, with the aim of obtaining a trustworthy output from them.

1.3 Scope

This document contains requirements and recommendations for assuring the quality and trustworthiness of digital twins, addressing all phases from concept to operation. The following topics are covered:

— maturity of the organizations developing and maintaining the digital twin
— the quality of the digital twin
— the risk of relying on the information provided by the digital twin
— operation and maintenance of the digital twin.

1.4 Application

This document applies to organizations involved in the procurement, development and operation of digital twins. The processes and requirements in this document are relevant for any digital twin of an asset or a system where it is essential that the results from the digital twin are trustworthy in order for the digital twin to be valuable.

It may be relevant for:

— asset operators: who request that a system supplier delivers a digital twin along with the asset/system
— system suppliers: who require a systematic approach to ensure and document that the digital twin will perform according to expectations
— sub-suppliers: who want to be able to deliver a qualified module to be integrated into a larger digital twin
— independent verifiers: who require a framework and a set of requirements to verify the digital twin against
— regulators: who require a framework to assure digital twins that relate to regulatory regimes.

For autonomous safety-critical systems, additional requirements from applicable safety standards, such as IEC 61508, apply.

1.5 References

The latest valid edition of each of the DNV reference documents listed below applies, see Table 1-1. For other standards and recommended practices, listed in Table 1-2, the edition valid at the time of publishing this document applies, unless dated references are given. Other external references are listed in the biblography, see [11.1].

Table 1-1 DNV documents

Document code	*Title*
DNV-RP-0317	Assurance of sensor systems for digital twins
DNV-RP-0497	Data quality assessment framework
DNV-RP-0510	Framework for assurance of data-driven algorithms and models
DNV-RP-0513	Assurance of simulation models
DNV-RP-A203	Technology qualification
DNV-RP-G108	Cyber security in the oil and gas industry based on IEC 62443
DNV-RP-O101	Technical documentation for subsea projects
DNV-RU-SHIP Pt.6 Ch.11	Digital features

Table 1-2 External standards

Document code	*Title*
ANSI/ISA 101.01	Human-machine interfaces
API RP 17N	Recommended practice on subsea production system reliability, technical risk, and integrity management
IEC 61508 series	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 62443 series	Industrial communication networks - Network and system security
IEC 81346-1	Industrial systems, installations and equipment and industrial products: Structuring principles and reference designation, Part 1: Basic rules
IEC 81346-2	Industrial systems, installations and equipment and industrial products: Structuring principles and reference designation, Part 2: Classification of objects and codes for classes
IEEE 1633	IEEE Recommended Practice on Software Reliability
ISO 14224	Petroleum, petrochemical and natural gas industries - Collection and exchange of reliability and maintenance data for equipment
ISO 15926 series	Industrial automation systems and integration-Integration of life-cycle data for process plants including oil and gas production facilities
ISO 8000	Data quality
ISO 8601	Data elements and interchange formats - Information interchange - Representation of dates and times
ISO/DIS 23247	Automation systems and integration - Digital Twin framework for manufacturing. Part 1 - 4: drafts published 2020
ISO/IEC 27001	Information technology - Security techniques - Information security management systems - Requirements
ISO/IEC/IEEE 12207	Systems and software engineering - Software life cycle processes

SECTION 2 DIGITAL TWINS AND KEY CONCEPTS

2.1 Introduction

This section introduces the digital twin (DT) concept and describes the different types of digital twins and their capability levels. Further, various key concepts fundamental to the qualification and assurance process are introduced.

The definition of a digital twin utilized in this document is as follows (Table 1-4):

A digital twin is a virtual representation of a system or asset that calculates system states and makes system information available, through integrated models and data, with the purpose of providing decision support over its life cycle.

The concept of digital twins was first described by David Gelernter's 1991 book *Mirror Worlds* /5/ and the term 'digital twin' was first coined by John Vickers of NASA in a 2010 roadmap report /6/. The digital twin concept consists of three distinct parts: the asset, the virtual representation, and the connection between the two. This connection amounts to the information transferred (automatic or manual) from the asset to the DT and information that is available from the DT to the asset and the operator.

A key principle is that the development of a DT should serve a clear purpose in order to provide value. Gartner uses the formulation 'improve business outcomes' when discussing the objective of digital twins /7/ and /8/. This RP focuses on decision support as a means to improve business outcomes. It should be noted that digital twins may be used for design, training, verification and certification purposes as well and this is considered to fall within the application of this RP.

Control systems, algorithms and embedded systems that are an integral part of the asset are not considered a DT but rather a cyber-physical system. In cyber-physical systems, physical and software components are deeply intertwined and interact with each other to enhance the functionality, performance, safety, etc. of the system. There are two reasons for making this distinction:

— The consequence of a failure in a cyber-physical system is typically higher than a failure in a digital twin, hence a different level of assurance is required.
— A cyber-physical system will typically be subject to the standards and regulation imposed on the asset that it is installed in.

A computation model from a cyber-physical system or control systems may be mirrored in a DT, for instance in a system-of-systems model, to replicate the response of the system. Also, there could be embedded systems on the physical asset that are required for the DT, for instance to provide the required sampling rate from instrumentation.

Conceptually, a DT may consists of some of the elements shown in Figure 2-1.

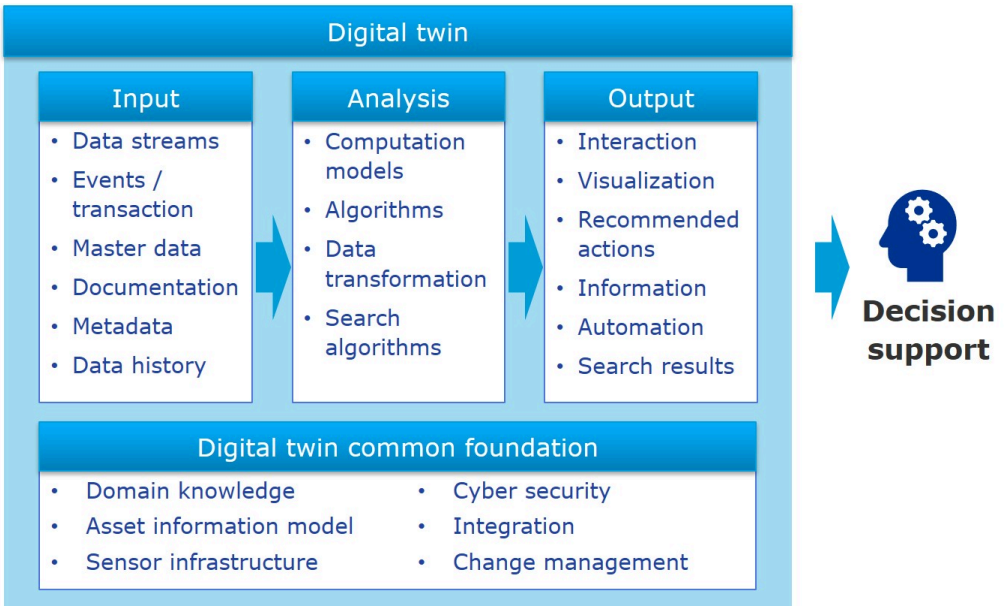

Figure 2-1 Elements of a digital twin

DTs may be used during the design phase of the asset or system to determine or test constructability, behaviour, performance, functionality, capacities, etc. before the physical product is realized. The design data, computation models, fabrication records, etc. that are established during the design and fabrication phases should be structured and contextualized in an asset information model to make them available and useful for the DT in operation, see Figure 2-2.

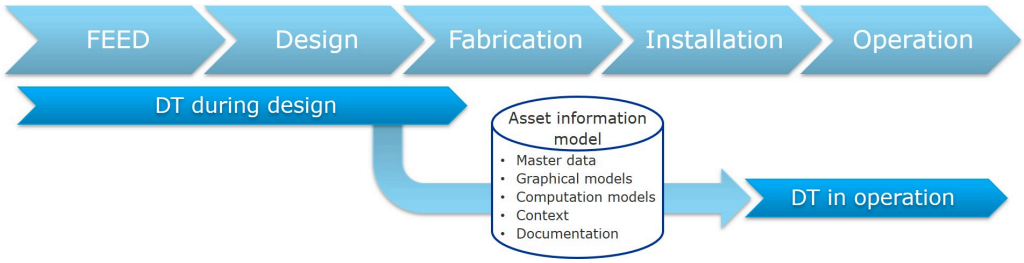

Figure 2-2 Connecting design and operations digital twins

2.2 Functional elements

In order to split the DT into more manageable pieces, the concept of functional elements is introduced. A functional element (FE) is defined as (Table 1-4):

A part or module of a digital twin with the purpose of supporting the user in making a key decision.

FEs may also be linked together to support a decision at a higher level. Every FE rests on its own domain, i.e. the key decision, the dashboard and quality indicator, computation models, asset information model, data streams and organizational elements, such as people and work processes, that jointly determine and influence the performance of the FE, see Figure 2-3. Although every FE has its own domain, some domain elements may be shared across multiple FEs, such as computation models and data.

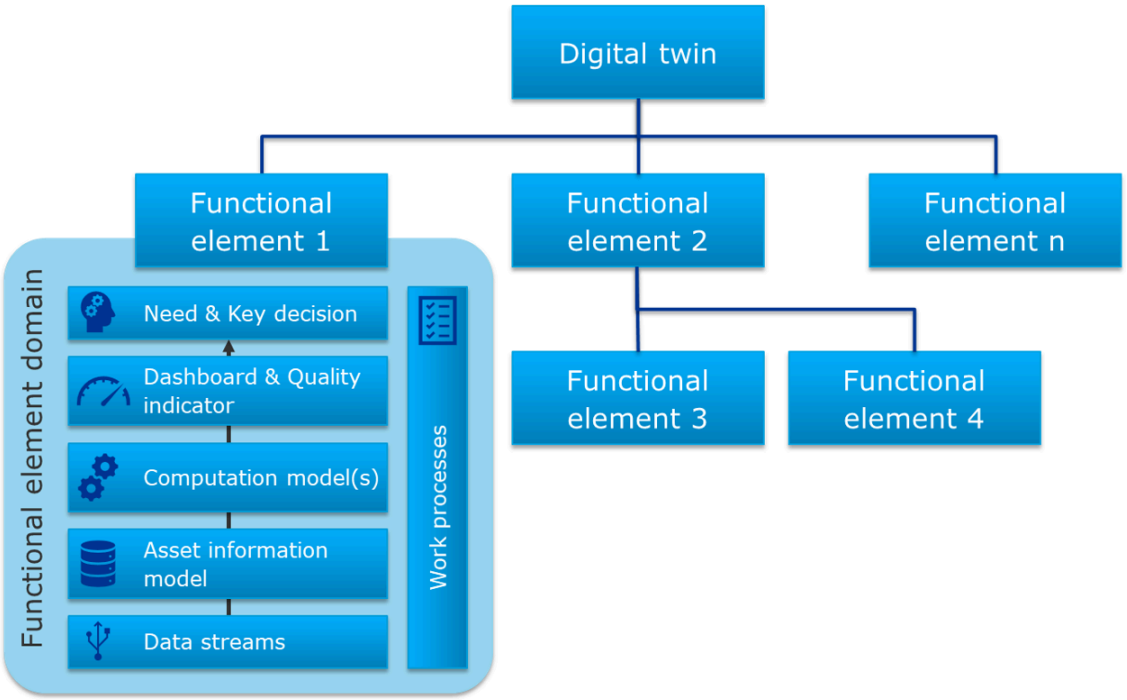

Figure 2-3 Digital twin as a collection of functional elements

The development of an FE will generally require multiple iterations to mature it to a point where there is a clear and common understanding between the target users, management and development team. Generally, multiple FEs will be developed in parallel and subject to prioritization and independent approval processes.

This RP covers cases where an FE relies on the output from another FE as input, hence there may be situations where a hierarchical dependency between FEs exists.

The principal qualification of DTs rests upon the qualification of each individual FE composing the DT. In turn, qualification of an FE requires an assurance process that evaluates all elements entering the FE domain.

2.3 Functional element capability level

Functional elements (FE) may be categorized into different capability levels, see /9/, as shown in Figure 2-4, where the capability increases for each level. These levels should be applied to each functional element, since a DT may contain FEs at any level. The capability levels may be used to describe the ambition of the FE and what the current capability is. The methodology presented in this document is applicable to all levels of FEs.

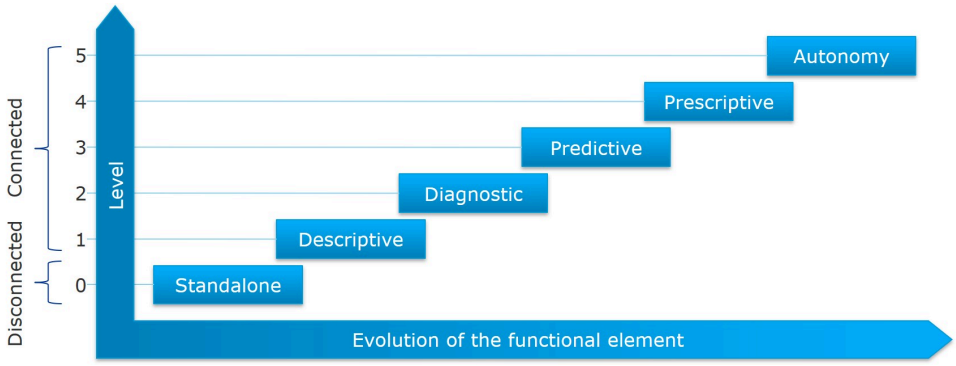

Figure 2-4 Evolution stages or capability of a functional element

There are two main categories of FEs for a system:

— Disconnected FE (level 0 - standalone): The system or asset does not exist or is under construction, i.e. the FE does not have a physical counterpart at this stage. The developer may use the FE to design and validate an asset where the models and output will be incorporated into an asset information model that may provide the foundation for the new functional elements or connected FEs. Disconnected FEs may also be used in the operation phase of an asset for training, planning new operations, modification projects, etc.

— Connected FE (levels 1-5): The FE now has a real counterpart that is typically connected to real-time data streams from the real system, corporate information systems or other external data sources. The levels indicate the capability of the FE, ranging from the ability to describe the current status, to the ability to predict future performance or conditions and to have autonomous functions.

The different levels are described in Table 2-1 and each level builds on the previously established capabilities.

Table 2-1 Capability levels for functional elements

Capability level	*Description*
0 - standalone	— The physical asset may not yet exist, no data streams are available from the asset. — The FE can describe and predict system behaviour based on manually entered data. — The asset information model has been developed and matured with the ability to provide a detailed description of the asset. It may contain contextualized and structured information, such as master data, graphical models, bill of materials, multidomain modelling (system-of-systems), etc.
1 - descriptive	— The FE can describe the current state of the system or asset. — Real-time data streams are available from the asset. — Describes the real system and provides status, alarms and events. — Ability to interrogate and provide information about the current and historical states.
2 - diagnostic	— The FE can present diagnostic information, such as health or condition indicators. — The FE can support the user with condition monitoring, fault finding and troubleshooting.
3 - predictive	— The FE can predict the system's future states or performance and remaining useful life. — Health and condition indicators are further enriched to support prognostic capabilities.

Capability level	*Description*
4 - prescriptive	— The FE can provide prescriptive or recommended actions based on the available predictions. — The FE evaluates the implications of each option and how to optimize the future actions without compromising other priorities.
5 - autonomous	— The FE can replace the user by closing the control loop to make decisions and execute control actions on the system autonomously. — The user may have a supervisory role over the FE to ensure that it performs as intended.

2.4 Criticality and confidence level

The qualification and assurance efforts for an FE depend on the criticality of the decision that the FE supports. The criticality of a key decision is proportional to the combination of the potential consequence of an incorrect decision and the likelihood of making that incorrect decision. The likelihood of making an incorrect decision is not easy to assess. Hence, this methodology uses two main factors as proxies: the availability of corroborating information from multiple sources, and the time available to critically evaluate the available information.

A criticality assessment for an FE results in assigning a confidence level from 1 to 3 to each FE, where 1 is low and 3 is high. The confidence level matrix is shown in Table 2-2. The confidence level is subsequently used to determine the applicable qualification and assurance requirements which the FE shall conform to. The number of activities and the requirements increase with higher confidence levels. These requirements are described in Sec.5, Sec.6, Sec.7, Sec.8 and Sec.9.

All the elements that are part of the FE domain [2.2] shall comply with the requirements of the assigned confidence level, including lower level FEs if relevant.

If the FE supports more than one key decision, the highest confidence level among those key decisions shall determine the assigned confidence level.

Table 2-2 Determination of required confidence level for a functional element

Basis for key decision	Typical FE capability level [1]	Potential consequence of wrong decision		
		Limited impact	Can cause delays, downtime or financial impact	Can cause major failures, accidents or environmental impact
The FE is one of several sources of information and decision making is not time constrained [2]	0, 1, 2	1	1	2
The FE is the primary source of information and decision making is not time constrained	3	1	2	3
The FE is the primary source of information and decision-making is time constrained	4	2	3	3
FE with automatic or autonomous functionality	5	2	3	3+ [3]

1) This is the typical capability level, see [2.3], or ambition for a functional element.
2) A decision is time-constrained when there is limited time to validate/corroborate it with other sources of information.
3) The requirements in this RP are insufficient for autonomous safety critical applications, so requirements from additional applicable standards shall be included.

2.5 Quality indicator

To ensure that the results from an FE are trustworthy and remain trustworthy over time, the concept of a quality indicator (QI) is defined. The QI is a self-diagnostic indicator that reports the quality of the provided results. In this context, the quality indicator refers to the accuracy or trustworthiness of the result, and not to the result itself.

The QI includes:

— a continuous assessment of the quality of the data sources, the computation models and potential failure modes
— a periodic assessment of any changes to the physical asset, performance of the computation models or data quality that have an impact on the digital twin.

The continuous assessment is typically automated, while the periodic assessment is typically performed manually. The QI may be presented as a 'traffic light' system, but other ways of communicating the quality indicator may be applied. The traffic light status may signify the following:

— green: the output/information is of sufficient quality for the key decision
— yellow: use the output/information with caution for the key decision as it may be of insufficient quality
— red: the output/information is of insufficient quality for the key decision.

See [5.2] for detailed requirements.

2.6 Technology readiness level

Technology readiness levels (TRL) may be used to indicate the maturity of technologies during the development or acquisition phase of a project or when comparing similar technologies. The purpose of TRLs is to enable a consistent, uniform discussion of technical maturity across different types of technologies. TRL is often used for physical systems but seldom for software-based systems. A TRL definition specific to functional elements has been included in App.D, where TRL 0 is an unproven concept and TRL 7 is a field proven concept. The use of TRL is optional in DT projects and the TRL is not linked to the confidence level or capability level.

SECTION 3 QUALIFICATION AND ASSURANCE PRINCIPLES

3.1 Introduction

This section describes the main principles that are applied for the qualification and assurance of digital twins. The RP uses the terms qualification and assurance of digital twins. These terms are related but not synonymous. Assurance refers to the evidence that a claim has been achieved, but does not specify how the claim and evidence should be developed and produced. Qualification refers to the process of producing the claims and evidence. The assurance process can be considered as the final step of the qualification process. This RP considers both these perspectives without assigning the specific activities and requirements to either category.

For an end user to have confidence in the results from a digital twin (DT), the following properties are required:

— valid and accurate data (data quality)
— accurate and trusted models and algorithms (computation model quality)
— presentation of meaningful results based on the relevant context (user interface)
— confidence that the DT is continually trustworthy (quality indicator)
— confidence that the DT mirrors the physical asset over time (change management).

In addition, a mature organization capable of developing and maintaining the DT over time requires:

— a systematic and scalable development and qualification process (work process)
— proportionality between the qualifying effort and the criticality of the FE (confidence level)
— a reliable and secure IT infrastructure
— an effective training process for new users
— a clear and versatile graphical user interface.

SECTION 4 PROCESS FOR QUALIFYING AND ASSURING DIGITAL TWINS

4.1 Introduction

This section provides a high-level description of the steps in the qualification and assurance process. This RP requires adherence to these process steps, which are described in detail in Sec.5, Sec.6, Sec.7 and Sec.8.

Qualification and assurance of digital twins are defined as (Table 1-4):

The process of providing evidence that the digital twin will provide trustworthy results, within well-defined limits and to a stated level of confidence, over time.

The DT qualification and assurance process consists of four main parts:

— Functional assurance: the qualification and assurance of each individual functional element (FE).
— Operational assurance: the monitoring of the performance of the FE and any changes to the physical asset to ensure that the DT and FEs remain qualified over time.
— DT platform assurance: the assessment of the platform that hosts the FEs, and the shared services it provides, to ensure that it is suitable for the purpose and that the interaction between the FEs is managed.
— organizational maturity assessment – the assessment of the organization's tools, processes, competence and capabilities relating to the development and maintenance of digital twins.

These parts are illustrated in Figure 4-1 and cover different dimensions of the development cycle. The FEs are the core of the DT and realize its business logic. The operational assurance ensures that the FEs remain qualified over time and continuously deliver the business logic.The DT platform hosts all the FEs and the shared services that enable DT operations. These parts are interdependent, so that changes to one will likely have an impact on the others. In addition, the figure singles out operations that occur in the physical realm of the DT. These operations correspond to triggering events, such as asset modification or improvement requests, and are highlighted in dark blue.

In addition, the organizational maturity refers to the degree to which an organization has processes and procedures in place for addressing organizational aspects of the DT, such as governance, management of digital infrastructures and architectures, and defined standards and metrics for measuring and recording the DT's performance.

The object of study shall be clearly defined with respect to the qualification and assurance process. This may include a list of elements that are part of the scope, such as the functional elements, use cases, data value chain, sensor systems, other building blocks of the DT, organizational units and suppliers.

Due to the complexity of developing, maintaining and operating a DT platform and its FEs, including the coordination between several parties, several roles are defined with associated responsibilities.

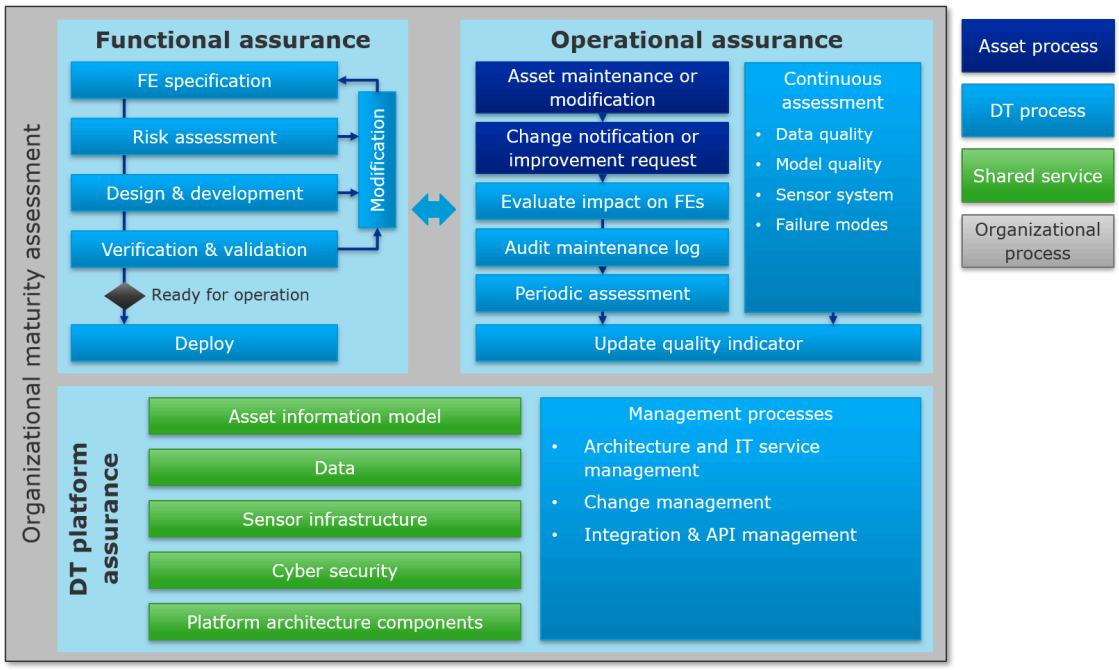

Figure 4-1 Digital twin qualification process

SECTION 5 ASSURANCE OF FUNCTIONAL ELEMENTS

5.1 Introduction

This section describes the requirements for the qualification and assurance process for a functional element (FE). This set of activities leads to an operable FE ready for deployment. Developers may use their preferred development method. Irrespective of the chosen method, each step of the process shall be documented, thus making the process and conclusions traceable. The required level of detail for the documentation tends to increase as the qualification process progresses. Figure 5-1 shows the process steps and decision gates for qualifying an FE.

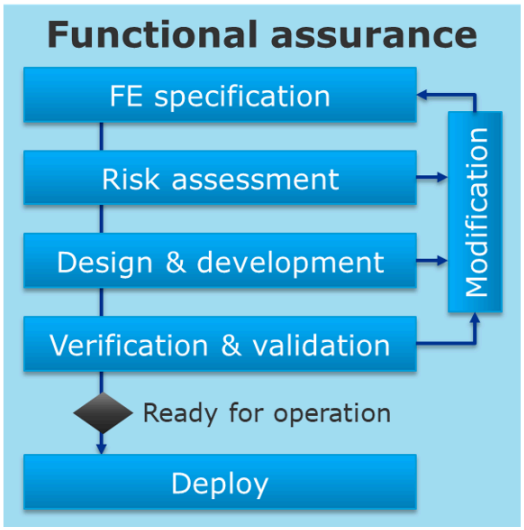

Figure 5-1 Work process for the development of a functional element

Developing an FE will typically require multiple iterations before the FE is mature enough to be implemented on the digital twin platform, see Sec.7. Consideration should be given to design modifications to improve safety, performance, longevity, cost and ease of operation, amongst other things. When implementing changes to the solution, the previous steps in the process shall be revisited to ensure that the FE specification and elements therein contained are coherent after the modification.

SECTION 6 ASSURANCE IN OPERATION

6.1 Introduction

The purpose of the assurance in operation process is to ensure that the DT remains trustworthy over time. A large and complex asset will typically see changes, modifications and maintenance work throughout its lifecycle that may have an impact on one or more of the FEs. The processes and requirements described in this section are designed for such large and complex assets. For smaller and less complex assets that do not have regular maintenance, the management processes of this activity may be simplified.

Any changes (modification or maintenance) to the asset shall be evaluated and the impact on the FEs identified and managed. Also, any degradation in the quality of the data used in FEs shall be identified and addressed in a timely manner. The quality of the output from the computation models shall be assessed and, if required, the computation models shall be updated or calibrated.

An operational assurance responsible shall be appointed, see [4.6]. This person shall be responsible for:

— ensuring that all FEs are subject to a periodic assessment procedure that is practical, serviceable and performed as scheduled, see [6.6]
— ensuring that FEs under development have followed the FE assurance process, see Sec.5
— ensuring that the periodic assessments for all FEs are performed in a coordinated manner
— periodically auditing the maintenance log and assess whether it has any impact on any of the FEs
— ensuring that the quality indicator is updated based on the periodic assessments.

The assurance in operation process is shown in Figure 6-1 and a description of each step is provided.

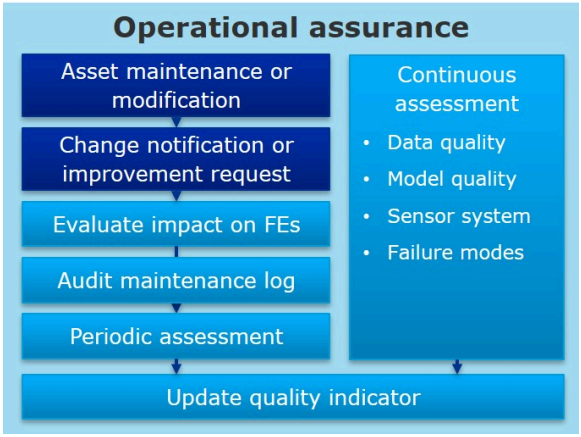

Figure 6-1 Work process for operational assurance

SECTION 7 ASSURANCE OF DIGITAL TWIN PLATFORM

7.1 Introduction

The DT platform is the environment that hosts the various functional elements (FEs) and provides the shared services and processes that are common to the FEs, see Figure 7-1. The horizontal boxes represent shared services that the platform provides, while the right-hand box represents the management processes required to ensure that the DT platform, with the hosted FEs, performs as specified.

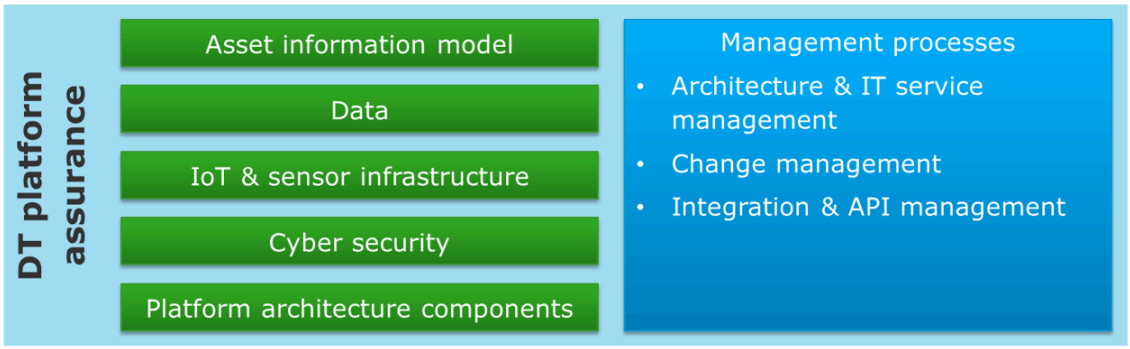

Figure 7-1 Digital twin platform services and work processes

SECTION 8 ORGANIZATIONAL MATURITY

8.1 Introduction

Organizational maturity refers to the degree to which an organization has tools, processes, competence and capabilities in place to develop and maintain digital twins over their lifetime. The methodology is inspired by the data management maturity model established by CMMI /11/. Organizational maturity includes organizational aspects of digital twins, such as governance, management of digital infrastructures and architectures, defined standards and metrics for measuring and recording DT performance. The maturity of the organization(s) developing and maintaining the digital twin, or parts thereof, shall be assessed by an independent party. The assessment shall be repeated regularly for the entire lifetime of the digital twin. The time interval between assessments is recommended to be two years but may be increased as the maturity of the organization increases. The DT platform responsible, see [4.6], shall plan and initiate these assessments.

SECTION 9 COMPUTATION MODELS

9.1 Computation model specifications

Computation models shall be qualified and of sufficient quality to provide FEs with trustworthy results. To this end, the quality of a computation model is determined by the degree to which it satisfies the specifications for the computation model. Specifications include, but are not limited to:

— the model's stated purpose and use case
— the model target accuracy or otherwise relevant measure of performance
— valid input ranges, combination of input
— data quality requirements
— the tolerance to known data quality issues that the model may experience in production
— response times, uptime
— assumptions
— model specific requirements.

Computation model quality metrics applicable to the computation model largely depend on the scope of the application at hand. It is not the scope of this RP to provide a list of model quality metrics, given the breadth of the topic. As an example, for a model which is tasked with estimating a continuous quantity, relevant metrics are those which represent deviations on a continuous scale, such as mean square error, mean absolute error or similar. For models predicting categories, relevant metrics may be accuracy, precision, recall or similar. The selection of the model quality metrics shall be documented with a clear and sound rationale linking the selected model quality metrics to the scope of the computation model, possibly with reference to broadly utilized scientific/industry practices.

CHANGES – HISTORIC

There are currently no historical changes for this document.

About DNV

DNV is the independent expert in risk management and assurance, operating in more than 100 countries. Through its broad experience and deep expertise DNV advances safety and sustainable performance, sets industry benchmarks, and inspires and invents solutions.

Whether assessing a new ship design, optimizing the performance of a wind farm, analyzing sensor data from a gas pipeline or certifying a food company's supply chain, DNV enables its customers and their stakeholders to make critical decisions with confidence.

Driven by its purpose, to safeguard life, property, and the environment, DNV helps tackle the challenges and global transformations facing its customers and the world today and is a trusted voice for many of the world's most successful and forward-thinking companies.

WHEN TRUST MATTERS