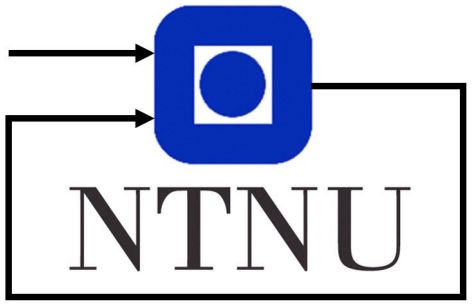
Digital Twin for Safety Demonstrations



Author:
Helene Pisani

Supervisor:
Prof. Mary Ann Lundteigen
Co-supervisor:
PhD. Ludvig Björklund

Specialization project
Department of Engineering Cybernetics
Norwegian University of Science and Technology

December 19, 2022

Preface

This project is part of the course TTK4551 in the two-year masters program in the Department of Engineering Cybernetics at NTNU. This is a 7.5 credit project.

This project has been carried out under the supervision of Prof. Mary Ann Lundteigen and PhD candidate Ludvig Björklund.

The report looks into a project by SUBPRO, centre for research based-innovation in the field of subsea production and processing, on developing a digital twin to demonstrate safety of an all-electric safety valve on subsea Christmas trees.

Executive summary

SUBPRO is conducting research on developing a digital twin to demonstrate the safety of an all-electric safety valve on subsea Christmas trees compared to the current state-of-the-art valve design.

The all-electric valve system consists of motor-driven valves, a safety controller, and a battery management system. The all-electric system is considered to have improved safety, reduced costs and increased reliability compared to the state-of-the-art electro-hydraulic system, but it is also more complex due to its components and software.

Digital twins can be used to simulate and analyze the performance of a manufacturing process or product in real time, improving efficiency and reducing downtime. Digital twins can also be used to perform safety demonstrations.

Safety demonstration is the process of proving that a system satisfies specific safety standards and requirements. This process is essential in the development and implementation of systems to guarantee their safety, reliability, and compliance with relevant safety standards, e.g. IEC 61508. Useful guidelines are NOG070 and NORSOK S-001. Safety 4.0 have introduced a new framework for safety demonstration of novel subsea equipment.

There is a proposed method for developing a digital twin of the gate valves for partial stroke testing to explore the potential benefits of using digial twins in development of subsea equipment and to determine their effectiveness in demonstrating the safety of novel systems in safety-critical applications. The process produces a working DT, but it still has improvements such as accuracy and more to be used for safety demonstration.

Table of Contents

List of Tables

List of Figures

Abbreviations

Abbreviation	Description
APS	Abandon Platform Shutdown
ASC	Actuation System Control
BMS	Battery Management System
CAD	Computer-Aided Design
D	Dangerous
DCV	Directional Control Valve
DHSV	Down Hole Safety Valve
DT	Digital Twin
DTI	Digital Twin Instance
DTP	Digital Twin Prototype
E/E/PE	Electrical/Electronic/Programmable Electronic
EPU	Electric Power Unit
ESD	Emergency Shutdown
EUC	Equipment Under Control
FMEA	Failure Modes and Effects Analysis
HDL	Hardware Description Language
HP	High Pressure
HSE	Health, Safety and Environment
IEC	International Electrotechnical Commission
IoT	Internet of Things
KISS	Keep It Stupid Simple
LP	Low Pressure
PFD	Probability of Failure on Demand
PSA	Petroleum Safety Authority
PSD	Process Shutdown
PST	Partial Stroke Test
PMW	Production Master Valve
S	Safe
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SOV	Solenoid-Operated Valve

1

Introduction

When introducing novel technology into safety-critical systems, like the systems that ensures strictly flow of hydrocarbons in the well, a structured process is needed to secure validation and verification of the proposed novel solution. The Norwegian regulations contains prescriptive requirements of systems which novel technology needs to meet, including the requirements given in NOG070 and IEC 61508 (1). The novel technology that will be presented and discussed are the new all-electric safety valves on subsea Christmas trees. A digital twin (DT) is proposed utilized to test and validate the new solution before put into practise. The DT will also be connected to the physical system during operation and be updated according to its physical counterpart.

1.1 Background

SUBPRO is a centre for research based-innovation in the field of subsea production and processing. The center is funded by the Research Council of Norway, nine industrial partners, and NTNU (7). The center launched in 2015 and has a planned duration of eight years. According to the SUBPRO annual report (7) their aim is to:

- reduce cost and complexity of subsea field developments
- enable development of new and more demanding oil and gas fields
- increase production and extend life of existing fields
- reduce environmental footprint of subsea field developments
- maintain safety levels

Safety 4.0 is a three-and-a-half year project funded by the Research Council of Norway and the project participants. The project aim to develop a safety demonstration framework to enable and accelerate the safe adoption of new cost-efficient subsea solutions (1). The project utilizes the all-electric Christmas tree in the development of the framework

with the help of pre-approved standards and guidelines recommended by the Norwegian Regulations.

Industry 4.0 is also affecting the oil and gas industry with integration of smarter systems. Sensor technology and increasing computational power have opened up for the use of DTs. Utilizing DTs for testing and safety demonstrations will increase the health, safety and environment (HSE), be more cost-efficient, material saving and environmental friendly.

SUBPRO has many research projects and one of them is on developing a DT to demonstrate that a all-electric safety valve for underwater systems are safe enough compared to the state of the art valve design. The research is in collaboration with Aalen university. The all-electric valves consists of motor driven valves, safety controllers and a battery management system (BMS). The PhD candidate working on this is developing a DT with the aim to test software for controlling the valve.

1.2 Problem description

The overall objective of this specialization is to give more insight into the construction of DTs to be useful for safety-demonstration.

Concerning this objective, the aim is to discuss and clarify:

- What do we mean by a DT?
- How to approach the modeling of a DT to be useful for safety demonstration?

The work divides into the following tasks:

- Present and discuss the following concepts: DT, safety demonstration, and safety demonstration applied to systems subject to functional safety.
- Describe the all-electric safety valve concept for subsea valve trees, including its functions and examples of failure modes. Give examples of safety concerns with the all-electric valve actuation system compared with the traditional electro-hydraulic system.
- Give examples of events where the subsea safety valves are closed with the basis of NORSOK S-001.
- Study and present the stepwise process proposed by Ludvig and Lundteigen (2022) and its application to the all-electric safety valve system. One or two submodels of the DT can be used as study cases.
- Identify potential improvements to the process and/or to the scope of modeling, using literature and own reflections from task 3.
- Propose ideas for further work as part of a master thesis.

1.3 Delimitations

This report has focused on parts and not the complete DT of the valve as it is still under development. Therefore the main focus has been on safety demonstration in the design phase of the DT and not so much the operation phase. The finished DT will consist of multiple parts of the all-electric Christmas tree and be fully integrated this the physical asset during operation.

1.4 Research approach

The main research approach used in this project is literature study. This study has been conducted by reading scientific papers on concepts, such as DT and safety demonstrations. In addition standards and guidelines have been used, especially IEC 61508, NOG070 and NORSOK S-001. The book published by DNV (1) safety 4.0 has been of good use. Conversations with supervisor and co-supervisor have been helpful. Participation in a PhD forum hosted by SUBPRO has also provided valuable insights.

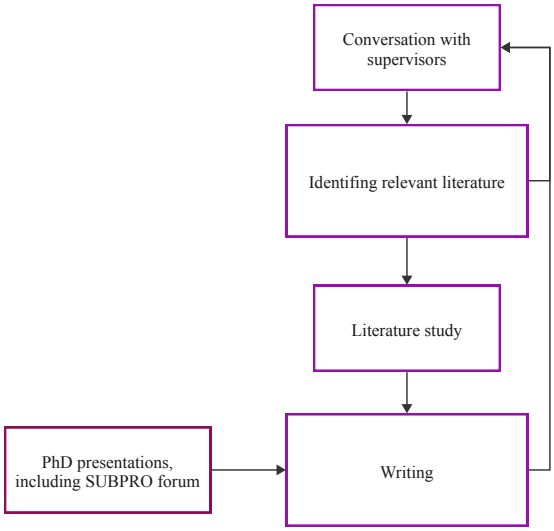


Figure 1.1: Research approach

1.5 Structure of the report

Chapter 2 introduces and compares the state of the art Christmas tree design and the new all-electric. Relevant standards and guidelines for development of novel functional safety systems offshore are presented. In chapter 3 the term DT is presented and discussed, together with information about safety demonstration. Then a stepwise process of developing a DT is presented and discussed. Lastly further work is proposed.

2

Subsea safety valves

A subsea Christmas tree is a valve stack placed on the bottom of the wellhead. On the subsea Christmas tree are the valves that control the flow of the hydrocarbons from the ground to the platform. The valves are called downhole safety valve (DHSV), production master valve(PMV) and production wing valve(PWV). The valves are normally open. Their main function is to maintain safety on the platform by closing and stopping the flow of hydrocarbons during emergencies. Safety is defined as freedom from risk which is not tolerable (8). Today the electro-hydraulic Christmas trees are the standard architecture world wide (1). Due to the increased digitalization and electrification of subsea equipment there is a proposal to make the valves all-electric. The new design will reduce cost, be more environmental friendly and be safer (9). The DHSV will still be hydraulic, only PMV and PWV are proposed changed to electric.

2.1 Electro-hydraulic Christmas trees

Figure 2.1 shows a simplified design of an electro-hydraulic Christmas tree. The figure is taken from the book published by DNV (1). A Christmas tree can have other designs and consist of multiple types of valves but they are not included in this figure because we want to address the safety valves: DHSV, PMV and PVW.

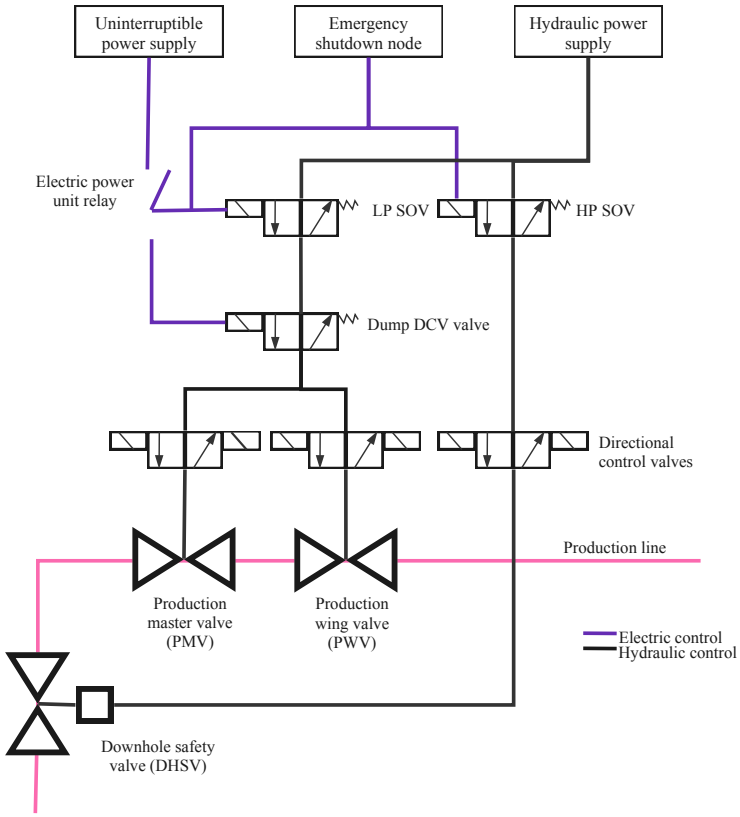


Figure 2.1: Architecture of electro-hydraulic Christmas tree (1)

The electro-hydraulic system described in the book published by DNV (1) works as follows: From below, the hydrocarbons first pass the DHSV, then the PMV and the PWV. The DHSV, PMV and PWV are hydraulic spring-return valves. They open and stay open by the pressure from the hydraulic fluid. The valves close when the hydraulic pressure is withdrawn. From topside, the hydraulic pressure goes through the solenoid-operated valves(SOV), through the umbilical and the directional control valves(DCV).

During normal operation, hydraulic pressure is available to the subsea Christmas tree, so the valves stay open. Normally and during a low-level emergency shutdown (ESD), the valves can be closed by using the DCVs.

During a high-level ESD and abandon platform shutdown(APS), the ESD node is used to de-energize the low-pressure (LP) SOVs and the electric power unit (EPU) relay. Following, the hydraulic pressure supply and the electric power supply disconnect. This de-energizes the Dump DCV valve, and the hydraulic fluid is drawn back, so the valves close. Lastly, the high-pressure (HP) SOV is de-energized. With this method, the process goes slower. Doing so makes the DHSV close last.

2.2 The all-electric Christmas tree

Figure 2.2 shows a generic architecture of an all-electric Christmas tree. The figure is a simplified version of the figure in Mahler et al. (2). The original contain more information than is necessary in the safety perspective. Only the PMV and the PWV are made electric, the DHSV will still be hydraulic and is therefore not in the figure. The box safety logic, battery and BMS and switch module are for safety's sake (2).

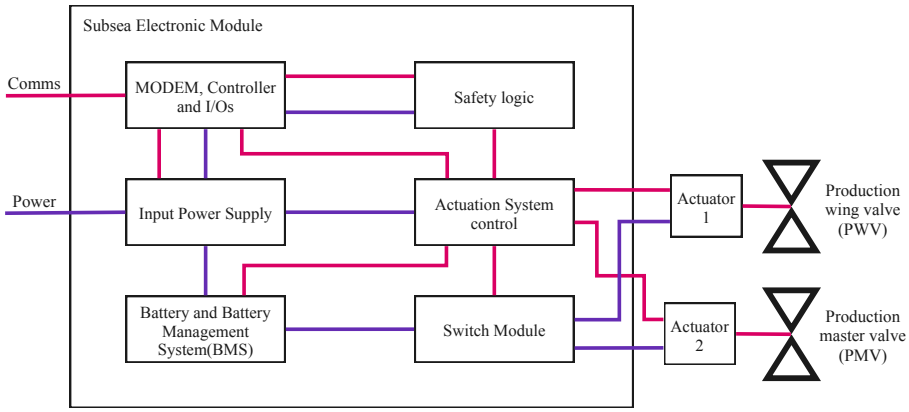


Figure 2.2: Architecture of all-electric Christmas tree (2)

In the all-electric Christmas tree, the power from topside comes through the input power supply. In addition, a battery is needed for uninterruptible power supply. If the power from topside is lost, then the battery will ensure power to the valves at all times (9). Along with the battery, a BMS is needed. The BMS monitors and controls the condition of the battery. The BMS is important for safety as it prevents failures in the battery.

The Switch Module on the Christmas tree is there to handle power to the actuators. To connect or disconnect each actuator separately (9). The switch unit is important as it prevents a common cause failure, i.e. "a failure that is the result of one or more events, causes concurrent failures of two or more separate channels in a multiple channel system, leading to system failure" (10). E.g a short circuit between the actuator and the battery, in this case, the working actuator must be closed (11).

The safety logic block observes the system status and commands the valves to their fail-safe position when necessary, e.g in the event of power loss (9).

The Actuation System Control(ASC) communicates with the topside controller via a safe communication link. The ASC also provides communications to the actuators and it monitors all of the safety-relevant system components.

Potential failure modes

A failure mode is a description of how a function can fail. Failure modes can divide into *safe*(S) and *dangerous*(D) and then into *detected* or *undetected*, shown in figure 2.3. The strength of the red indicates how critical the failure is. A dangerous failure prevents the system from executing the safety function when required (10). Safe failures are failures that do not prevent the safety function of a system from being executed and are therefore not considered critical. Safe failures can still cause complications and inconvenience but do not directly threaten the safety of users and surroundings. An undetected failure is a failure that we cannot detect with traditional diagnostics. Detected dangerous failures are less critical than undetected dangerous. This is because other measures can be taken to maintain safety when the failure is known.

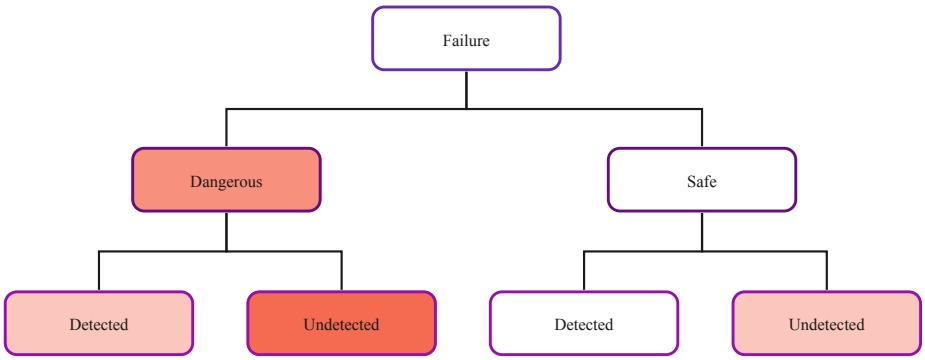


Figure 2.3: Failure modes

The paper by Mahler et al. (9) have performed a failure modes and effects analysis(FMEA) of the all-electric Christmas tree. A FMEA is used to find the causes of potential failures and evaluate their consequences. As a result, four main failure modes of the valve for isolating the well are presented:

Failure mode	Failure type
Fail to close	D
Fail to open	S
Internal leakage	D
External leakage	D

Table 2.1: Failure modes of valve

In the all-electric Christmas tree, failure of the individual components can lead to failure mode of the safety valves.

If the battery fails the control of the valves are lost. The BMS is included to prevent failures of the battery but if the BMS fails, the safety function of the system will fail. An example of a failure in the battery is thermal runaway. Thermal runaway is when a chemical reaction happens in one of the battery cells and this leads to overheating of the battery and in worst case fire.

The motor provide a force to the actuator to either close or open the valve. If the torque is too big the valve shaft can be damaged which then can lead to leakage.

A shortcircuit in an actuator can lead to failure mode *Fail to close* or *Fail to open*. The risk of this is mitigated using redundancy. If one actuator fails the switch module disconnects the failed actuator and provide power to the other one working.

Topside and subsea communicate with a digital communication link. The digital communication link can freeze and this can also lead to failure (1).

2.2.1 Electro-hydraulic versus all-electric

The design of the electro-hydraulic valve is very simple and rarely fails (1). The all-electric control system proposed in the paper (9) provides ”improved HSE, reduced costs and increased safety and reliability compared to the electro-hydraulic system”. However, the new all-electric system is more complex as it exist of multiple components and includes software. The technology is still novel and there are safety concerns regarding this. The Petroleum Safety Authority (PSA) requires the new system to meet the same safety standards as the electro-hydraulic (1).

A safety concern with the all-electric valve is the need for a battery. The battery has its own failure modes. To mitigate the failure of the battery a BMS is included.

All-electric Christmas trees enable new test cases and increases the diagnostics. The valves are rarely used, they are almost always in open position. However, failure can happen while they are in this position and go unnoticed until a shutdown is needed, leading to unwanted events. On the all-electric Christmas tree, partial stroke testing (PST) can be used to test the functionality of the safety valves. This type of testing involves closing the valve a small amount and observing the amount of force needed to close it. This can help determine if there are any obstructions or issues with the valve that may prevent it from functioning properly. PST can be done monthly to ensure the that the safety valves work without impacting the production.

2.3 Governing standards and guidelines

2.3.1 IEC 61508

The International Electrotechnical Commission (IEC) is an international organization that develops and publishes standards for electrical, electronic, and related technologies. It is a leading global organization in this field. Their objective is to promote international cooperation concerning standardization on electrical and electronic fields (10). IEC 61508

is a standard for functional safety, achieved by safety-related systems that are primarily implemented in electrical and/or electronic and/or programmable electronic (E/E/PE) technologies (10).

IEC61508-0 describes functional safety as part of the overall safety relating to the equipment under control(EUC) and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures (10).

The functional safety is executed by a safety instrumented function(SIF). The IEC 61508 gives advice on how to maintain functional safety. It is a crucial tool to utilize when dealing with functional safety and especially when introducing novel technology.

2.3.2 NOG070

The NOG070 is a guideline on the use of IEC 61508 and IEC 61511 for the sake of the Norwegian petroleum industry, where IEC 61511 is a standard on functional safety of safety instrumented systems for the process industry sector. The main purpose of the guideline is to standardize and simplify the use of IEC 61508 and IEC 61511 (12). While the IEC 61508 and IEC 61511 gives a risk-based approach to identify the performance requirements, NOG070 proposes a set of predefined performance requirements for functions that are already identified as necessary by national and international standards used by the Norwegian petroleum sector (12).

The guideline provides the probability of failure on demand(PFD) and based on this, the safety integrity level (SIL) of different SIFs. The PFD is the probability of the system not working when we want it to execute the safety function (10). The PFD is calculated in NOG070 by using data from experience. The SIL tells us how much we can rely on the system to execute its safety function when needed (10). Table A.13.9 in NOG070 summarizes the SIL requirements for isolation of the subsea well (12). The PMV and PWV make the secondary isolation barrier of the production line and are given SIL 2.

2.3.3 NORSOK S-001

NORSOK S-001 is a national standard for technical safety (3). The purpose of the standard is to reduce the time and cost of development and operation of petroleum installations on the Norwegian continental shelf.

Included in this standard are hazard identification, risk analysis and evaluation, risk treatment and performance requirements. The standard describes the execution of ESD on the platforms and when the different safety valves will close and is therefore helpful in this article. The purpose of the ESD system is to prevent the escalation of abnormal conditions into a major hazardous event and to limit the extent and duration of any such events that do occur (3). The process safety system is part of the ESD system, and it is here the safety valves are involved.

ESD Hierarchy

The ESD system is needed in multiple scenarios, from shutting down only the production system to shutting down the whole platform. The shutdowns are triggered by either push of a manual button or the detection of a dangerous event, such as a fire in a hazardous area.

The ESD functions are put in a hierarchy shown in figure 2.4 (3). The ESD levels are divided into three where the APS is the highest, ESD 1 is in the middle, and lastly ESD 2. The process shutdown (PSD) is initiated by ESD 2. The hierarchy works so that a higher ESD level should initiate a lower one and a signal on a certain level should never initiate shutdowns or actions on higher levels (12).

An example of such an action is shutting safety valves. ESD valves shall isolate and sectionalize the process segments in a fast and reliable manner to reduce the number of released hydrocarbons in the event of a leak.

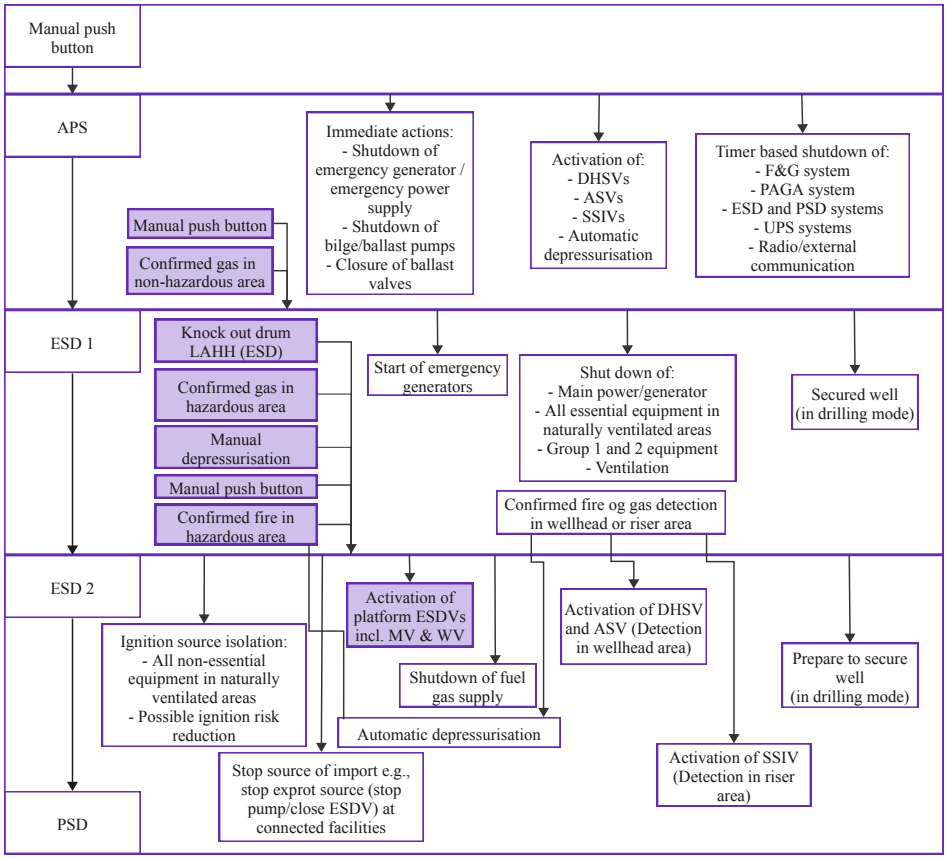


Figure 2.4: ESD hierarchy (3)

2.3.4 Examples where the safety valves are closed

The safety valves are closed in the action ”activation of the ESDV incl. MV and WV”, which is highlighted in the ESD 2 box. The highlighted signals trigger the action:

- Manual push button

- Confirmed gas in non-hazardous area
- Knock out drum LAHH (ESD)
- Confirmed gas in hazardous area
- Manual depressurization
- Confirmed fire in hazardous area

The action is also initiated in the event of APS or ESD 1.

3

Digital twin and safety demonstration

3.1 Digital twin and industry 4.0

Industry 4.0, also known as the fourth industrial revolution, refers to the current trend of automation and data exchange in manufacturing technologies, including the use of advanced technologies such as artificial intelligence, the Internet of Things (IoT), and machine learning (13). This trend is leading to the development of more complex, software-dependent systems that are capable of greater levels of automation and intelligence.

As part the digitalization and the industry 4.0 initiatives, development of DTs has increased. DTs can be used to simulate and analyze the performance of a manufacturing process or product in real-time, allowing manufacturers to identify and address potential issues before they arise. This can help improve efficiency, reduce downtime, and ultimately, enhance the overall performance of the manufacturing process.

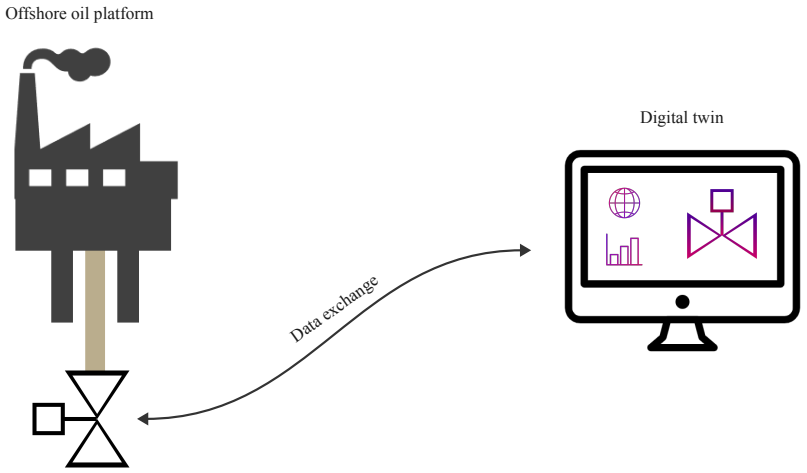


Figure 3.1: The DT is on a computer while the physical valve is placed on the platform. They are linked through data exchange.

There exist many definitions of what a DT is. A DT defined by DNV (14), is a dynamic virtual representation of a physical object or system across its lifecycle, using real-time data to enable understanding, learning, and reasoning. Due to the increased advancement of information and communication technologies and digitalization, DTs are utilized more often.

The book by Vickers et al. (5) addresses how we earlier only could have any knowledge about a system or object by being right next to it looking at it. Over the years, engineers have found ways to have more and more knowledge about systems. Both about their design and functions. Firstly by making national standards for products made it easier to mass produce and repair. In the last half of the twentieth century, information started to get digital. Some sparse computer-aided design(CAD) illustrations were the beginning of the DT (5). These illustrations were just a static representation of the object. Today we can make detailed simulations about the system, not only before it is set up but also during its operation time.

3.1.1 Level of integration

Kritzinger et al. (4) distinguishes the DT into three forms based on the level of data integration between the physical asset and the DT. Figure 3.2 visualizes the data flow between the three DTs and the physical asset. The figure is inspired by the figures in the article by Kritzinger.

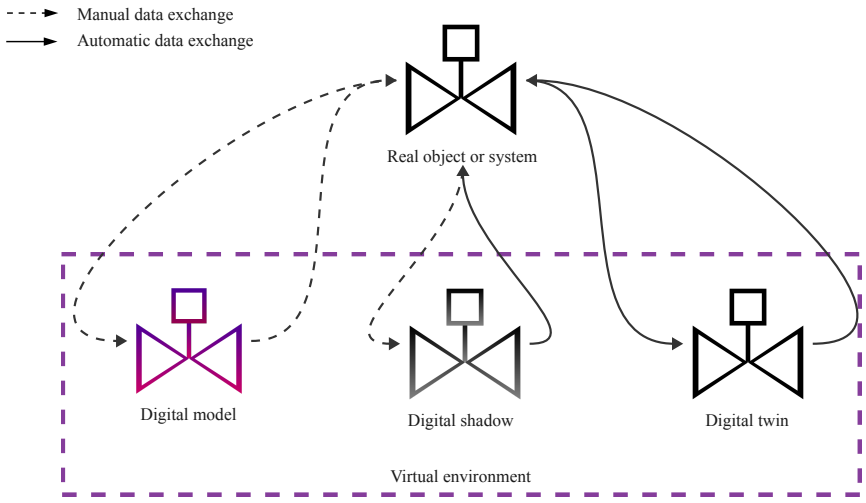


Figure 3.2: Different types of DTs based on level of integration (4)

The three forms of DTs described in Kritzinger et al. are:

The first form of DT is a simple digital replica of a physical asset. It is called a *digital model* and typically only includes basic information about the asset, such as its shape, size, and location. It may not be connected to any real-time data or information about the asset's performance or condition.

The second form of DT is called a *digital shadow*. It involves some level of data integration between the physical asset and the DT. In this case, the DT may be connected to sensors or other sources of real-time data about the asset's performance or condition. This allows the DT to provide more detailed information about the asset and its behavior.

The third form of DT is a fully integrated *digital twin*, in which the DT is closely connected to the physical asset and is updated in real-time with data from sensors and other sources. This type of DT can provide a highly detailed and accurate representation of the asset and its behavior, and can be used for a variety of purposes, including predictive maintenance, performance optimization, and scenario planning.

Vickers et al. (5) propose a different way of classifying DTs, using the terms *digital twin prototype*(DTP) and *digital twin instance*(DTI). In their approach, a DTP is a virtual model representing a physical object and the requirements to produce a physical version that duplicates the virtual version. In other words, a DTP is a virtual representation of an object used to design and develop the physical version of that object. On the other hand, a DTI is a DT that is linked to a specific physical product. This means that the DTI represents a specific physical product, and it remains linked to that product throughout the life of the product. The DTI provides real-time data and information about the physical product. It can be used for various purposes, such as predictive maintenance, performance optimization, and scenario planning. Overall, both approaches to classifying DTs are useful in different contexts. Depending on the specific use case and the goals of the DT, one approach may be more useful than the other.

3.1.2 Digital twin through the product lifecycle

Systems are not always perfect on the first try and often require trial and error to develop and improve (5). This can be costly, inefficient, and even dangerous if not managed properly. Additionally, systems are not static and tend to evolve over time as they go through their product life cycle. The product lifecycle presented by Vickers et al. (5) contains four main stages presented in figure 3.3.

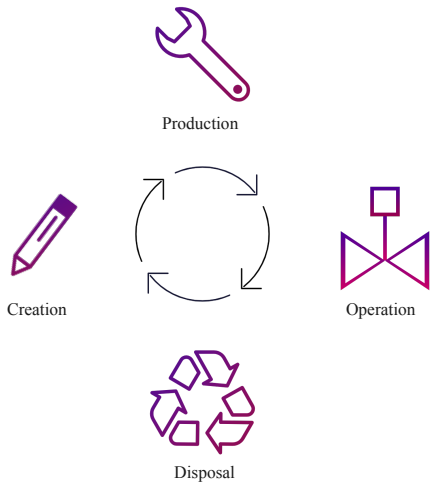


Figure 3.3: Product lifecycle (5)

During the creation and design phase, the engineers identify the concept and the overall scope of the system. To support this process, standards and guidelines, such as IEC 61508 and NOG070, provide frameworks and guidance for designing and developing robust and reliable systems. These standards and guidelines help ensure that the system meets specific performance and safety criteria and can make designing and developing more robust systems easier. The next step is to create a DTP to represent the physical asset.

Using a DTP to simulate the behavior of an asset can provide valuable insights and information about the asset (15). Testing the all-electric valve in the real world is more costly because it requires physical equipment and may be limited to testing only certain parameters, such as a single valve size. In contrast, a DTP allows for testing a wider range of parameters and settings, providing greater flexibility and insight.

In addition to testing correct functionality, injecting parameters to initiate failure modes in the system's DT can give valuable insight. This process involves simulating the system's behavior under various conditions and inputs and applying specific parameters known to cause the system to fail. By simulating these failure modes and observing the system's behavior, developers can evaluate the system's reliability and identify potential weaknesses or vulnerabilities.

The next phase is the production phase. In this phase, the DTP is used to produce a physical version of the asset, which is then linked to the DTI. The design of a system is not

always physically possible. Therefore the design usually changes during the production phase, and because of these changes, undesirable system behaviors can arise (5). By using a DTI during production, changes can first be implemented and tested on the DTI before implementing it on the physical system.

The third phase is the operation phase. In this phase, the DTI is used to provide real-time data and information about the physical asset, and to support various operations and activities related to the asset. It is first here it is called a DT by Kritzinger et al. (4) definition. Changes during the operation phase can first be implemented and tested on the DTI before implemented on the physical asset.

The last phase is the disposal phase. In this phase, the physical asset reaches the end of its useful life and is decommissioned or retired. The DTI is also retired in this phase. Data from the DTI can be stored and analyzed to make better systems in the future systems.

3.2 Safety demonstration

Safety demonstration is defined as documentation, based on evidence and structured reasoning, that adequate safety criteria are specified and met (1).

It is the process of demonstrating that a system meets certain safety criteria and standards. This is an essential step in developing and deploying systems, as it helps to ensure that the systems are safe and reliable and meet relevant safety criteria and standards.

Demonstrating that a system is safe and reliable provides evidence that the system will not pose a risk to people, property, or the environment. Safety demonstration is important when developing novel technology. A safety demonstration of the all-electric Christmas tree is important before it can be put into use.

3.2.1 IEC 61508

In the context of safety demonstration, IEC 61508 (10) plays an important role by providing a set of requirements and guidelines that systems must meet to be considered safe and reliable. The standard defines the different SILs that systems must achieve.

The IEC 61508 describes the lifecycle of a product from a safety perspective. The safety lifecycle is used to systematically address all the activities necessary to achieve the required safety integrity for the safety functions performed by E/E/PE systems (10).

The lifecycle contains 16 steps that divide into six categories. Where the first describes planning and development. This involves defining the safety requirements and objectives for the system and developing a safety plan to meet these requirements. The next category is design and integration. The system is designed and integrated, and safety-related components and functions are selected and implemented.

The safety demonstration is typically performed in the following category: verification and validation. This category involves testing and evaluating the system to ensure it meets the safety requirements and objectives defined in the planning and development phase.

The system is manufactured, installed, and put into operation in the production and operation category. The maintenance category contains ongoing maintenance and support of the system, including regular inspections, repairs, and updates. Lastly, decommissioning category involves removing the system from service and disposing it appropriately.

3.2.2 Safety 4.0

Due to the trend of increased advanced technologies in manufacturing such as artificial intelligence and the IoT, more complex and software-dependent systems are developed.

The phrase ”Keep it stupid simple” (KISS) is often used in engineering and safety to emphasize the importance of simplicity in design. The idea behind KISS is that simple, straightforward designs are often the most effective and the easiest to understand, maintain, and operate (1).

The new software-dependent systems may be more cost-efficient, safer, and environmentally friendly, but the increase in complexity can jeopardize these features. This lead to the Safety 4.0 project.

Safety 4.0 is a three-and-a-half year project funded by the Research Council of Norway and the project participants. The project aim to develop a safety demonstration framework to enable and accelerate the safe adoption of new subsea solutions (1). The framework includes how to deal with diverse types of failures, increasing complexity and uncertain assumptions. Like the Norwegian regulations, the Safety 4.0 refers to international safety standards, e.g IEC 61508.

The project utilizes the all-electric Christmas tree in the development of the framework with the help of pre-approved standards and guidelines recommended by the Norwegian Regulations.

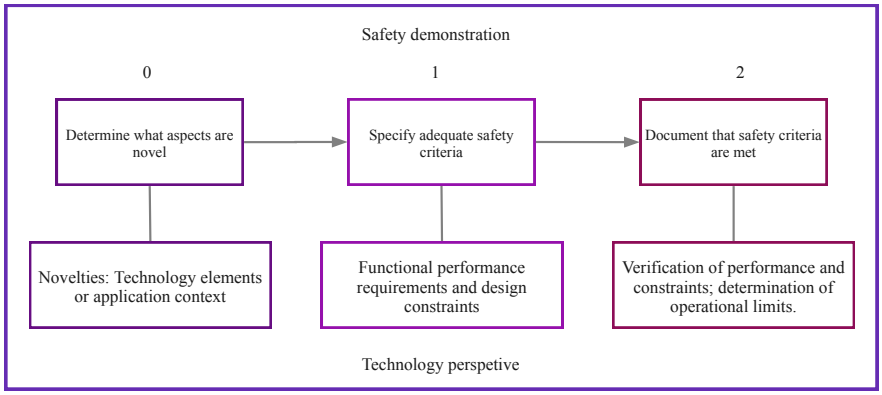


Figure 3.4: Safety demonstration in technology perspective (1)

Safety demonstration according to safety 4.0 (1) is based on three steps which are shown in figure 3.4:

- 0. Determine novel aspects of a solution.
- 1. Specify adequate safety criteria.

- 2. Provide arguments and evidence that these are met.

Combined with the three steps, the safety demonstration process divides into three subprocesses, each with a different focus and perspective. Dividing makes it easier to identify where the novelty occurs and where to put in the effort.

The subprocesses are the *activity* perspective, the *strategy* perspective, and the *technology* perspective. The technology perspective is most relevant for developing the all-electric Christmas tree.

The technology perspective asks, ”is the technology safe?”. It focuses on the technical aspects of the system, including the hardware and software components used. The technical equipment must pass the performance requirements and operational constraints needed for the activity to be safe and reliable (1).

3.2.3 Digital twin for safety demonstration

The SUBPRO project aims to develop and implement a DT of an all-electric Christmas tree and to use this DT for the safety demonstration of the system.

Some benefits of using a DT are (16): DTs provide a safe and controlled environment for testing and evaluating the safety of a system. By simulating the system's behavior on a computer, engineers can test and evaluate the system's safety without exposing it to real-world hazards.

It is efficient and cost-effective to simulate safety demonstration using a DT. Engineers can test and evaluate the system's safety without building and operating the physical system. This can save time and money and allow engineers to test and evaluate the system's safety more quickly and efficiently.

DTs allow for real-time monitoring and evaluation of the system's safety. Because DTs are digital models, they can be updated and modified in real-time based on new information and data. This allows engineers to monitor the system's safety in real-time and to make changes to the system as needed to ensure its continued safety.

A challenge of using DTs for safety demonstration is ensuring that the DT accurately represents the behavior of the physical system. This can be difficult, as not all test scenarios may be realistic enough on a computer, and the DT may not capture all the nuances and complexities of the physical system.

To address this challenge, Björklund et al. (6) have developed a stepwise process for designing a DT for safety demonstration. The process will be presented and discussed in the next chapter.

4

Stepwise process on developing a digital twin

Björklund et al. (6) propose a method for developing a DT of gate valves for PST. The motivation for this project is to explore the potential benefits of using DTs in the development of subsea equipment. DTs can be used to test and evaluate the behavior of these systems. The DT can simulate the performance of the valve during PST, which are commonly used to assess the safety and reliability of the valve.

The proposed methodology for developing a DT of a gate valve focuses on creating a computationally inexpensive model that can accurately capture the relevant behavior. This will enable the testing of diagnostics and controllers without the need for physical experimentation. Additionally, the evaluation of the proposed methodology will help to determine its effectiveness in demonstrating the safety of novel systems in safety-critical applications. This research aims to expand the possibilities of using DTs to assess the safety and reliability of subsea equipment (6).

The paper uses the term DT, referring to the definition by Kritzinger et al. (4). However, at the current stage of development, the DM of the gate valve is not yet connected to the physical asset. Once the model is complete and has been validated, it can be connected to the physical asset to create a DT.

The process will be presented before any criticisms or limitations of the proposed methodology is discussed.

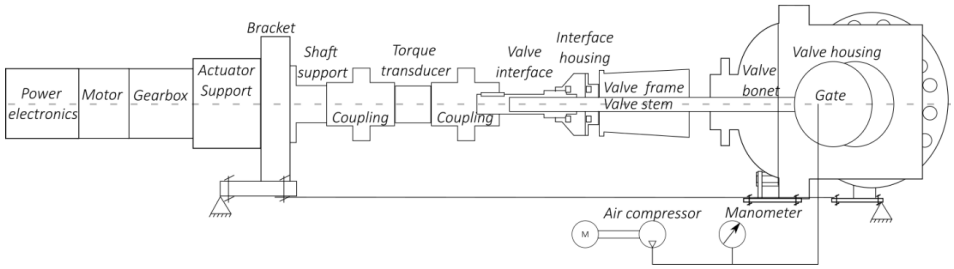


Figure 4.1: Technical drawing of valve (6).

4.1 Steps of the process

The proposed sequential process of developing a DT for PST is presented in figure 4.2 (6). An important aspect of designing the DT is making it not too complex. The DT should only include what is necessary to represent the physical asset to perform a safety demonstration. This is crucial to assure the DT is computationally efficient and simple. All the steps in the method are taken to ensure a rational development of the DT to be used for safety demonstrations (6).

Analysis
The process starts with analyzing the physical system and finding out which parameters are needed to model the system.

The drawing of the system is shown in figure 4.1 (6). The gate valve is moved by rotating the valve stem.

The test cases for PST include both open-to-close and close-to-open movements of the valve. The close-to-open movement is not a common occurrence in normal operation, but the test can still provide valuable information. In this case there will be a much bigger difference between the pressure on each side of the valve. This differential pressure help the developers determine the friction force on the valve (6).

Parameter Evaluation
Which parameters to include in the model are then evaluated. This step is important in order to keep the DT simple and limit computational costs. Parameters that do not significantly contribute to the desired behavior of the valve during a PST can be discarded.

In order to focus on the key aspects of the valve's behavior during a PST, the researchers have decided to only include the valve stem and gate in the modeling. This allows to specifically examine the effects of friction on the torque required to open and close the valve.

Other key behaviours are backlash and breakaway torque. Backlash refers to the small gap or clearance between the components of a mechanical system, such as gears in a gear train. The breakaway torque is the amount of torque applied before friction is overcome and the valve moves.

Define the physical relations between parameters
The next step is to evaluate the physical relations between the parameters. E.g for the valve design, the torque give rotational energy which is transformed to linear energy and helps open or close the valve.

Design digital twin
The next step of modeling the system in a virtual environment e.g. Simulink.

Calibration
The model is then calibrated with data from experimental testing of the test case close-to-open, to help tune the parameters to obtain a model similar to the physical asset. The result of the tuning in comparison with the experimental data can be seen in figure 4.3.

Validation
Data from experimental testing is also used for validation of the DT. E.g. the measured angular velocity is used to make a simple PI controller that controls the input torque.

Validation successful
If the validation is successful the DT is ready to be deployed for testing of diagnostic software.

Deploy digital twin for diagnostics
The final step is to implement the DT.

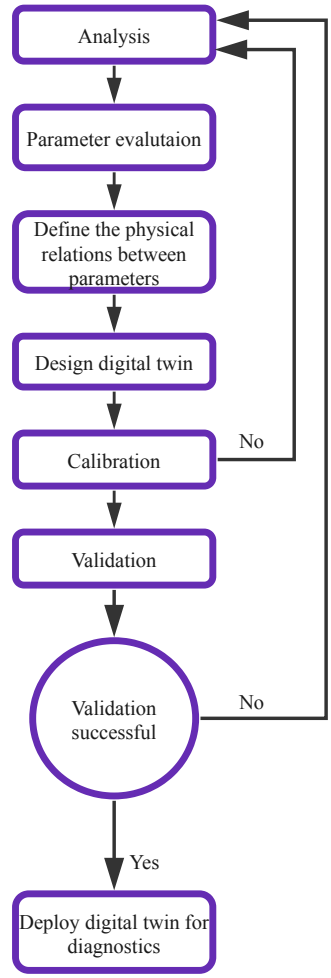
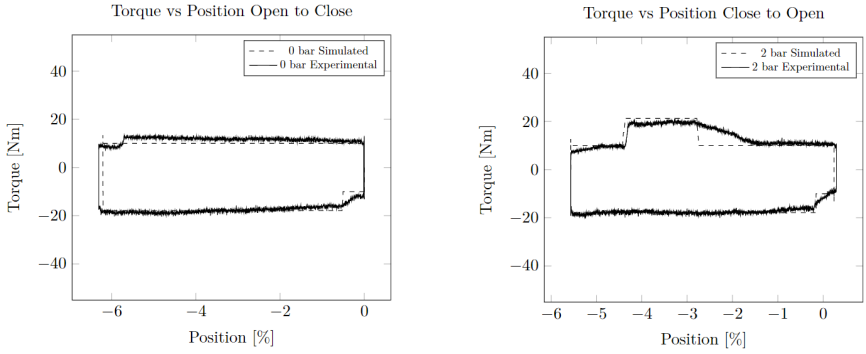


Figure 4.2: Stepwise process of developing a DT (6).

4.1.1 Results

The paper concludes with a good working DT. A simple model is capable of capturing much of the behavior of PST (6). This is verified in figure 4.3 (6) where the result of the DT is compared to the result from real-life testing. The selected parameters is sufficient. The paper suggests there is potential to expand the usefulness of the DT by capturing neglected behavior and incorporating more detailed modeling. The DT was developed using simplifications to make it computationally efficient, but incorporating more detailed modeling could enable the DT to provide additional insights and information about the behavior of the gate valve.



(a) Torque applied with a initial differential pressure of 0 bar.

(b) Torque applied with a initial differential pressure of 2 bar

Figure 4.3: Simulated torque compared to experimental torque (6).

4.2 Shortages of the process and potential improvements

4.2.1 Defining scope

The process jumps straight into analyzing the system. There should be a step before the analysis to determine the scope and purpose of the DT. The analysis is not easily performed without a clear scope.

4.2.2 Short descriptions

Overall, the different steps are not fully explained how to perform. The description of the process steps is short and should be more detailed.

4.2.3 Limited testing

The DT is only tested on some parameter combinations. For the DT to be used for all different kinds of valves, multiple parameters combinations should be tested.

The DT is only tested on a limited parameter range, and it is unclear how it would perform outside of this range. E.g, the friction force may be much higher or smaller in reality and this is not tested in the DT. The DT was developed using simplifications and assumptions, e.g. the relationship between torque and pressure is assumed to be linear. However, if in reality as the torque force increases, the relationship could become nonlinear. In this case the DT developed is not a sufficient representation of the physical valve.

A likely scenario is an obstruction of the valve or something else causing the valve to be stuck. A high torque would have to be applied to close the valve. This could worst case lead to damage of the valve. This should be tested to ensure that the DT is able to accurately model the behavior of the physical system.

4.2.4 Failure modes

The goal of the project is to develop a DT that can be used for safety demonstration purposes. In safety demonstration, it is essential to evaluate the safety of a system and consider potential failure modes.

The process do not include how to model failure modes. Modelling failure modes and the consequences of them could give valuable information. One of the benefits of using DT is that it is safer than real life testing. Especially when testing failure modes.

The DT should be able to simulate failure modes and demonstrate how the system respond. It should be tested that the system holds it SIL requirement.

A step for evaluating how to incorporate failure modes should be part of the process. Determine which additional parameters are needed to model the failure modes. This could help to improve the DT's ability to demonstrate the safety of the system and to evaluate potential failure modes.

4.2.5 Not universal process

The process cannot straight forward be applied to any other systems. E.g the battery in the all-electric valve is also going to be made a DT of. The most commonly used method for modeling a battery is not as intuitive as the method used to model the gate valve. A battery contain chemical reactions, which are difficult to model accurately. Therefore, the usual method of modeling a battery is to create a circuit model using resistors and capacitors. The model will then give the same outputs as a battery.

One challenge in the process is the step **parameter evaluation**, which is difficult because the parameters used in the battery model do not correspond to the actual parameters of the real-life battery. This issue should have been addressed in the process to ensure that the modeling remains accurate.

4.2.6 Test data

The DT was developed using data obtained from physical testing of the all-electric valve. The DT was calibrated and validated using this real-life data. A purpose of using a DT is to not have to do physical testing.

However, it is not easy to evaluate uncertain physical parameters like the friction coefficient without real-life data. On the other hand, other measures for validation exist, e.g. DNV (14) presents methods for qualifications and assurance of DTs.

5

Conclusion and further work

A DT is a digital replica of a physical object or system that can be used for various purposes, such as simulating the object's or system's performance, predicting its behavior, or optimizing its operation. DTs are created by integrating data from sensors, simulations, and other sources into a digital model of the object or system. The use of DTs can help organizations improve efficiency, reduce costs, and enhance the performance of their physical assets.

The stepwise process presented by Björklund et al. (6) lays the foundation for developing a DT. However, the process needs to be optimally described to produce a sufficient DT. There still need experimenting and testing to develop a good enough DT for safety demonstration. Especially considering implementing failure modes for fault detection.

Including the improvements proposed in chapter 4.2 the article proposes further work. E.g it can be challenging to determine the optimal amount and types of tests to perform. Further work could be done to develop a testing environment for testing and verification of the DT and the software. The interface needs to be standardized and intuitive in order to be usable for testers that may not have advanced technical expertise. This is an area that I plan to explore in my master's studies.

Bibliography

[1] K. Berg, A. Hafver, O. I. Haugen, K. Kvinnesland, M. van der Meulen, T. Myhrvold, F. B. Pedersen, B. Søgård, M. A. Lundteigen, N. A. Zikrullah, A. Falck, R. Flage, C. B. Nyvik, and H. Kim, *Demonstrating safety of software-dependent systems*. Høvik, Norway: DNV AS, 2022.

[2] C. Mahler and M. Glaser, "Application of functional safety in all-electric control systems," in *Underwater Technology conference*, Bergen, Norway, 2018.

[3] NORSOK, "NORSOK S-001 Technical safety," *Standard, NORSOK*, 2021.

[4] W. Kritzinger, M. Karner, G. Traar, J. Henjes, and W. Sihn, "Digital twin in manufacturing: A categorical literature review and classification," 2018.

[5] M. Grieves and J. Vickers, *Transdisciplinary Perspectives on Complex Systems*, 2017.

[6] L. Björklund, M. Glaser, S. Imle, G. Skofteland, and M. A. Lundteigen, "Design of a digital twin of gate valves for partial stroke testing," 2022.

[7] SUBPRO, "SUBPRO annual report 2021/2022," 2022.

[8] ISO/IEC, "NEK ISO/IEC Guide 5," 2014.

[9] C. Mahler, M. Glaser, S. Schoch, S. Marx, S. Schluenss, T. Winter, J. Popp, and S. Imle, "Safety capability of an all-electric production system," 2019.

[10] IEC, "IEC 61508, functional safety of electrical/electric/programmable electric safety-related systems," *Standard, IEC*, 2010.

[11] T. Winter, M. Glaser, B. Bertsche, S. Imle, and J. Popp, "Analysis of an all-electric safety subsea actuation system architecture," 2020.

[12] O. NORGE, "070 – Offshore Norge application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry," *Guideline, NOG*, 2020.

[13] M. Ghobakhloo, “Industry 4.0, digitization, and opportunities for sustainability,” 2020.

[14] DNV, “Qualification and assurance of digital twins,” 2020.

[15] A. Parrott and L. Warshaw, “Industry 4.0 and the digital twin,” *Deloitte*, 2017.

[16] J. Wang, L. Ye, R. X. Gao, C. Li, and L. Zhang, “Digital twin for rotating machinery fault diagnosisin smart manufacturing,” 2018.