Achieving More Responsible Drone-Use by Means of Blockchain Technology

A Case Study for the NVWA

MOT26010: Master Thesis

A.D. Poelman - 4475283

[This page is intentionally left blank.]

Achieving More Responsible Drone-Use by Means of Blockchain Technology:

A Case Study for the NVWA

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **Management of Technology**

Faculty of Technology, Policy and Management

by

Armando Dyon Poelman

Student number: 4475283

To be defended in public on August 30th 2021

Graduation committee

Chairperson	: Prof. dr. ir., P.H.A.J.M. (Pieter) van Gelder, Safety & Security Science
First Supervisor	: Dr., A.Y. (Aaron), Ding, Department of ICT
Second Supervisor	: Prof. dr. ir., P.H.A.J.M. (Pieter) van Gelder, Safety & Security Science
External Supervisor	: Ir. R. (Rob), Broekman, NVWA

[This page is intentionally left blank.]

Preface & Acknowledgements

Already at the start of my Bachelor Degree in Aerospace Engineering, I've been fascinated by drones and its current applications. The fast pacing technology has shown great potential in various application domains and excited me to do this research. Throughout my study period I experienced interest in IoT management and contacted A.Y. Ding, an expert in the field of ICT. After discussing my interests and background briefly, consensus about a topic in the field of drone management was obtained. Moreover, A.Y. Ding introduced me to the Netherlands Food and Consumer Product Safety Authority (NVWA), a governmental agency that uses drones for inspection purposes in agricultural practices. Ultimately, a research in combination with an internship was formed. The internship lasted for 6 months and started in February 2021. Due to the on-going pandemic, visiting the office and getting a realistic grasp of the organisation was difficult. For this reason, the internship mostly included desk research at home and conducting interviews by phone or online. The benefit of online meetings were fast contacting of third parties and colleagues out of office. My external supervisor was very helpful and provided all the resources required for doing this research. The first period of the research I experienced difficulties in finding a fitting scope of research. The great range of on-going projects such as Drone2Go made it hard to find a fitting research scope while being dense enough for a thesis of only 6 months time. Also, open issues such as dynamic legal framework concerning drones in the Netherlands made the start of the research quite complex. After a lot of fine-tuning and weekly meetings, a refined focus on security and privacy issues was found. This focus coincided greatly with my electives and led to the following research.

Throughout the process, I experienced great support from both my internal supervisor from the TU Delft as well as my external supervisor at the NVWA. I first would like to show my gratitude to A.Y. Ding from the TU Delft for introducing me to the NVWA and accepting my research proposal. His enthusiasm, positive attitude and critical feedback during our weekly meetings kept me focused and reduced stress over the research period. I received great freedom and steering throughout the process and would definitely recommend A.Y. Ding to other students doing research in the field of ICT. Subsequently, I want to thank R. Broekman of the NVWA who gave me the opportunity to do this internship. He provided me with the resources required and gave helpful information about the organisation and its current obstacles. Besides, his enthusiasm for drone technologies and believe in my professional skills stimulated me to deliver a high-quality report. Additionally, I want to show appreciation to the committee chair P.H.A.J.M. van Gelder who provided useful feedback during the start, midterm and at the end of the research. His expertise in safety and security science has led to useful feedback and tips to increase the quality of the analyses. Besides, his positive attitude and excitement about the topic was very much appreciated. Lastly, I wish to thank the team of the NVWA and all individuals who participated in the interviews and thereby created value to this research. Their input and insights in the subject helped me narrow the scope of this report and helped me deliver the final design.

A.D. Poelman - 4475283
Delft, August 2021

[This page is intentionally left blank.]

Executive Summary

With the advent of a smart society and an era of connectivity, there remain a numerous amount of challenges yet to be solved. One of the key IoT innovations analysed in this research is known as Unmanned Aerial Systems (UAS). UAS, or drone technologies, allow carrying out repetitive and dangerous tasks with almost no human intervention or supervision (Fernández-Caramés, Blanco-Novoa, Froiz-Míguez, & Fraga-Lamas, 2019). The advent of drone utilisation in both public and civil domains has led to application areas such as real-time monitoring and surveillance, parcel delivery, search and rescue missions (e.g. ER), remote sensing in agriculture and multiple other application domains (Valavanis & Vachtsevanos, 2015). However, the fast pacing development of interconnected devices and systems has outrun the human understanding and experience of usage, imposing challenges with regards to technical security, trust and of course privacy (Coetzee & Eksteen, 2011). Subsequently, most drones are limited to computing, storing and sharing data, making them vulnerable to adversarial attacks. A need for a more responsible adoption of drone-use exists and must be fulfilled with care. To this, a blockchain-based solution is proposed.

The focus of this research is on a Dutch independent agency part of the Ministry of Agriculture, Nature and Food Quality, called the Netherlands Food and Consumer Product Safety Authority (NVWA). They have been actively using drones since 2017 and their main tasks consist of supervision, risk assessment and risk communication with the goal to protect the human and animal welfare (NVWA, n.d.). An explorative research approach was taken whereby the current bottlenecks experienced by the NVWA were identified and visualised, by means of desk research and semi-structured interviews. Subsequently, the sociotechnical effects of the use of drone detecting services by the NVWA were identified to obtain the key values for a responsible redesign. In this way, the role of the values, an understanding of the roles of institutions realizing these values, and the stakeholder engagement is understood. After identifying the open issues and conflicting values, a redesign phase began with the trade off between three mitigating security techniques.

Blockchain technology is found to be the most suitable security technique in this research and fills in the 'lack of transparency' gap which is crucial for a responsible redesign. Although it hasn't reached full maturity and could induce undesired delays, it increases the security level of the organisation significantly and takes into account the key values security and privacy. Moreover, the data managing method allows users to validate, maintain and synchronize the content of a transaction ledger which is replicated across the other users in the network (Tapscott & Tapscott, 2017).

The solution has proven to work in existing literature and automotive contexts and is therefore generalisable in multiple on-going projects of the NVWA. Subsequently, the novel data managing method could be used as for revenue models such as digitised inspections. This indicates future growth options and potential competitive advantages. All in all, the benefits outweigh the uncertainties of this technology and it is believed that a blockchain-based solution will be the next big step to achieve more responsible implementation of drones.

Contents

List of Figures

List of Tables

1

Introduction

With the arrival of a fourth industrial revolution - known as ’Industry 4.0’ or ’Smart Industry’ - the boundary between the physical and digital realm has faded away greatly. Trends in high-tech like Artificial Intelligence (AI) and Internet-of-Things (IoT) start transforming industries greatly, disrupting existing systems, and eventually creating novel innovative solutions (Griffiths & Ooi, 2018). Numerous organisations follow this trend of digitisation and start adopting SMART technologies such as drones in their daily practices. Drones are agile, efficient and easy to use. Subsequently, it is a IpT devoce hence can constantly gather and monitor data in real-time. However, along with the ’infinite’ amount of opportunities this technology offers, there remain several challenges and threats that should be addressed. The fast pacing development of interconnected devices and systems has outrun the human understanding and experience of usage, imposing challenges with regards to technical security, trust and of course privacy (Coetzee & Eksteen, 2011). More specifically, most IoT devices are limited to computing, storing and connecting data, making them vulnerable to adversarial attacks. Subsequently, an increasing amount of users and smart devices yield substantial security challenges such as device vulnerabilities, mismanagement and misconfiguration.

IoT, one of the disruptive trends related to drones, is used as an umbrella keyword for covering various aspects related to the extension of the Internet and Web into the physical realm by the extensive deployment of spatially distributed devices with embedded identification, sensing and/or actuation capabilities (Miorandi et al., 2012). The emerging vision for an IoT industry will connect billions of objects to the Internet, having enormous social and economic implications. An era of digitisation arrived whereby ’automation’ is the new standard.

According to Brous, Janssen, & Herder (2020), IoT adoption in the industry brings incredible benefits ranging from better data quality giving real-time and accurate insights for strategic managers, to improved flexibility of services and trend analysis of historical data over time. The benefits for organisations are mainly derived from the availability of more diverse information, real-time collected and translated after generation. It allows devices to ’learn from their mistakes’, increase efficiency and to reduce the working time needed.

Now in this research, the focus is on arguable one of the most trending IoT applications of Industry 4.0; Unmanned Aerial Systems (UAS). UAS, or drones, are an emerging form of IoT devices used by various parties for surveillance, crime investigation, search and rescue operations, locating stolen goods, recreation, and surveying land and infrastructure. This value-adding system has gained popularity in a wide variety of applications, commercially as well as recreational, and is anticipated to expand its use throughout civilian airspace. (Jafary et al., 2019) Many organisations start to adopt this innovation as it improves their competitive position and overall efficiency. Moreover, (recreational) drones are able to capture, monitor and share data, both creating and destroying value for existing systems.

Applications of drones differ per country and will be narrowed down to the case of the Netherlands. More specifically, the case of the Netherlands Food and Consumer Product Safety Authority (NVWA), an independent agency part of the Ministry of Agriculture, Nature and Food Quality, is being analysed. Already since 2017, the NVWA has been experimenting and expanding its application domains by the use of drones. One of their activities consists of scanning large parcels, identifying illegal dumped cadavers such that the spread of diseases among animal population can be prevented. Before, this was done manually hence very labour-intensive and time-consuming. The arrival of parcel-scanning drones disruptively changed their way of inspecting parcels and led to faster identification rates and more accurate results. (NVWA, n.d.) Another activity consists of the detection of illegal fisheries, i.e. detecting fykes and fishnets. This usually done by inspectors detecting fykes and fishnets from a boat. Again, scanning large areas is very labour-intensive and time-consuming. Besides, in some cases this can lead to dangerous situations for the inspectors. For this reason, a project is set up for detecting illegal fykes and fishnets by means of drones. In this way, a faster detection rate is obtained while enhancing the inspector's safety level. (Custers, Oerlemans, & Vergouw, 2015) (NVWA, n.d.)

1.1. Open Issues and Existing Approaches

Now, one might argue if adopting this 'life-changing' and 'convenient' innovation is solely sunshine and rainbows. By using drones, an increase in dependency is experienced hence increase in risk in case of failure. Drones are able to monitor and share personal data 24/7 to the cloud and can hence be vulnerable to attacks. Although cloud service providers claim their systems are secure and safe, some should reconsider 'giving up privacy' for more comfort and convenience. A study by Aydin (2019) quantifies the public acceptance of drones by conducting a survey to both internal and external stakeholders. The results had shown that people tend to be unaware of future drone applications, and many current applications. Aydin (2019) recommends that public and private institutions should collaborate to develop risk mitigation and response strategies to minimise risks and better the roll-out. In this way, the image of drones being 'killer machines' or 'privacy interrupters' might be reframed in a positive way.

According to Coetzee & Eksteen (2011), three different obstacles exist currently in the Netherlands; the conservative legal framework, lack of resources and a lack of transparency in the process. The technique has proven to work however remains to be slow and/or without protocol, making traceability hard and leading to a lower trustworthiness. Chen et al. (2015) propose a distributed approach for IoT device management and service composition from a social network point of view. A method is introduced to encapsulate the heterogeneous IoT devices by web services which regards all different components as uniform service modules with in- and output interfaces. It allows users to gain access to devices using the method in a unified and flexible way. By letting the IoT devices work in relationships and unifying them, more governance and control over the devices present is obtained, hence increased transparency. This method could be adapted to the heterogeneosity in drone-use such that a unified access system is formed.

A paper by Bassi et al. (2019) analyses the risks concerning the use of UAS and proposes a tool for managing data protection risks raised by drones. More specifically, GDPR-abiding drones are designed by means of flight operation maps. Through the design of flight maps, operators can choose the best air corridor based on a so-called privacy by design principle of the GDPR. The aim of designing and tailoring fly zones is to present a win-win approach to data protection issues, engineering challenges and risk management for the threats posed by drones in use. The study has set a first step in constructing flight operation maps and proposes a solution for data protection issues.

Furthermore, Jafary et al. (2019) assesses the drone's cyber security level by means of assurance methods and standards. Since UAS are cyber-physical systems, they will be subject to cyberattacks indicating protection is needed for the hardware, software and of course data involved. The study expands on existing cyber risk management standards and presents a stop light chart method adapted from the safety domain. A quantitative method that considers attacks, their likelihood and impact, and alternative deterrent and defensive countermeasures, thereby enabling the comparison of alternative mitigation strategies through a countermeasure allocation problem, is proposed. This framework informs the users of the relative cost involved and its effectiveness of reducing total risk.

Blockchain Approaches

A possible method of tackling the security and lack of transparency issues addressed is by using blockchain technology. The first implementation of this technology was performed by a group of researchers under the name Nakamato with the introduction of Bitcoin. (Tapscott & Tapscott, 2017) The goal of this research was to link transactions in a tamperresistant manner such that the formed network allows the examination of the transaction history, thereby preventing the double spending problem. It is a data managing method that allows users to validate, maintain and synchronize the content of a transaction ledger. (Popovski, Soussou, & Webb, 2014)

A research by Demir, Turetken & Ferworn (2019) shows how blockchain can act as a transaction medium between interacting parties. The paper proposes a tamper-free ledger to store a history of transactions and act as an insurance record for motor vehicles. This would benefit in two ways; proving insurance but also as evidence in case of an incident. The study analyses the case of motor vehicles but might as well be generalised in the case of (autonomous) drones. In case of incidents occurrence with drones, the ledger's tracing back abilities would benefit greatly.

Another research done by Khan, Byurn & Park (2020) in the field of CCTV, presents a blockchain-based system to guarantee the trustworthiness of the stored recordings. Moreover, it allows authorities to validate whether a video has been altered, helping discriminate fake from real data and ensuring the surveillance cameras' authenticity. This validating system hence shows there is an option to trace back actions and stresses transparency. The work process is in this way transparency and fake or personal data may be filtered accordingly. Since the essence and issues of CCTV and drones respectively are similar, this might be an interesting option for this research. Besides, it increases both transparency and security in the system, which tackles the open issues adressed before.

Alladi, Chamola, Sahu & Guizani (2020) found the same and looked into the applications of blockchain in unmanned aerial vehicles. The study reviews applications in UAV networks such as network security, decentralised storage and surveillance, and discusses the various challenges to be addressed in the integration of blockchain. Similar issues were found and a blockchain solution was proposed. The study was very concise but nicely coincides with the case of the NVWA and can serve as an interesting input for the design phase of the report.

1.2. Problem Statement

From the existing literature it became clear that many open issues remain to exist for implementing drones in the Netherlands. Issues range from the restricting legal framework to the lack of transparency and trust in the process. Moreover, security and privacy concerns arise with the growth of drone-use. There is a need for transparency and traceability in the work process such that the uncertainty factor is resolved. By doing this, developing projects can cross the prototyping phase and an increased adoption rate can be achieved. Subsequently, both users and non-users are then convinced the technology is reliable and enhances their key values. In other words, when the adoption is done more responsibly, an increased adoption rate of drone-use could be achieved.

The major knowledge gap of this research can hence be formulated as the ***lack of transparency*** in the process of acquiring data by means of drones. Lack of transparency leads to low trust in the system and is closely connected to values such as privacy and security. Perhaps if the focus is transferred to the communication of the work process in stead of the technology, a more responsible adoption rate is achieved such that more application domains in the Netherlands can be enriched with drone technologies.

1.3. Research Objective & Questions

From the introduction it became clear that there is still a gap in research to be filled; exploring the absence of transparency in the work process such that a more responsible adoption rate is achieved.

To achieve the objective stated above, a research question is compiled.
The **main research question** can be formulated as follows:

”How to improve the work process of drone detecting services used by the NVWA such that a more responsible adoption rate is achieved?”

To help find an answer to the main research question, the following **sub-questions** must be answered accordingly;

SQ1: Current Process

While the knowledge gap is clear, first a visualisation must be given of the current process including activities, process flows and bottlenecks. This explorative section will assist in mapping the bottlenecks and forms a base for the redesign phase. The sub-question can therefore be listed as follows;

SQ1: *What does the current process of implementing drone detecting services by the NVWA look like?*

SQ2: Added Value

Since there remains an uncertainty factor among authorities and citizens, it is beneficial to map the overall value added by the implementation of drones in societal practices. This includes looking at the benefits, negatives of the technology, potential trends and of course plausible ’hidden’ barriers. The second sub-question is therefore stated as follows;

SQ2: *How do drone detecting services create value for the NVWA and what are its main barriers?*

SQ3: Socio Technical Mapping

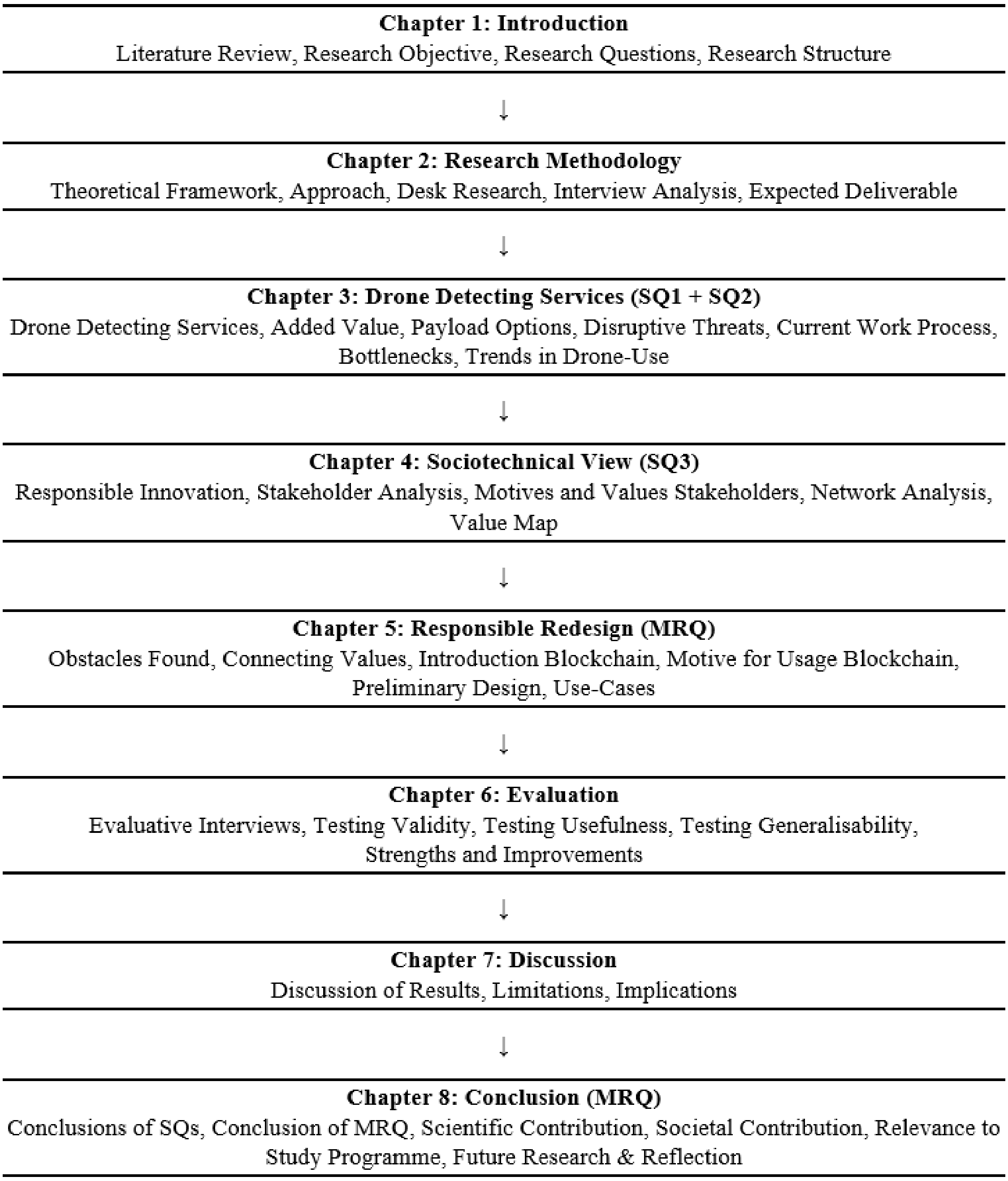
Lastly, a Socio Technical Value Map is constructed such that all stakeholders involved and their interests, values and power are identified. This will lead to the construction of an ethical framework or value map which can be used to propose a responsible redesign of the work process and adoption of drone detecting services. Key conflicting values are mapped and used as an input for the redesign phase. The last sub-question is hence stated as follows:

SQ3: *What are the sociotechnical effects of the use of drone detecting services by the NVWA?*

In this research, the case of the Netherlands Food and Consumer Product Safety Authority (NVWA) will be analysed whereby drones are mainly implemented for agricultural surveillance (inspections) and measuring purposes (supervision). Relating back to the knowledge gap identified before, the main goal of this research is *to contribute to the introduction of an enhanced implementation process of drones, such that a more responsible adoption rate is achieved.*

1.4. Report Outline

The structure of this research can be found in detail in the figure below.



Chapter 1: Introduction

Literature Review, Research Objective, Research Questions, Research Structure

↓

Chapter 2: Research Methodology

Theoretical Framework, Approach, Desk Research, Interview Analysis, Expected Deliverable

↓

Chapter 3: Drone Detecting Services (SQ1 + SQ2)

Drone Detecting Services, Added Value, Payload Options, Disruptive Threats, Current Work Process, Bottlenecks, Trends in Drone-Use

↓

Chapter 4: Sociotechnical View (SQ3)

Responsible Innovation, Stakeholder Analysis, Motives and Values Stakeholders, Network Analysis, Value Map

↓

Chapter 5: Responsible Redesign (MRQ)

Obstacles Found, Connecting Values, Introduction Blockchain, Motive for Usage Blockchain, Preliminary Design, Use-Cases

↓

Chapter 6: Evaluation

Evaluative Interviews, Testing Validity, Testing Usefulness, Testing Generalisability, Strengths and Improvements

↓

Chapter 7: Discussion

Discussion of Results, Limitations, Implications

↓

Chapter 8: Conclusion (MRQ)

Conclusions of SQs, Conclusion of MRQ, Scientific Contribution, Societal Contribution, Relevance to Study Programme, Future Research & Reflection

Figure 1.1: Report Outline

2

Research Methodology

Section 2.1 elaborates on the theoretical framework chosen for this research. This is followed by the approach taken, including the desk research, interviews and the corresponding analysis. Afterwards, the expected deliverable for this thesis is shortly discussed.

2.1. Theoretical Framework

In order to answer the research questions established, the Design Science Research Method (DSRM) by Peffers, Tuunanen, Rothenberger & Chatterjee (2007) is used. According to Hevner (2007), design science research is motivated by the desire to improve the environment by the introduction of new and innovative artifacts and the processes for building these artifacts. Peffers et al. (2007) elaborates on Hevner (2007) his theory and evaluates a methodology for conducting design research in information systems. This so-called DSRM method presented, includes principles, practices and procedures required to carry out the research. A distinction is made between six activities as seen in the blocks in Figure 2.1.

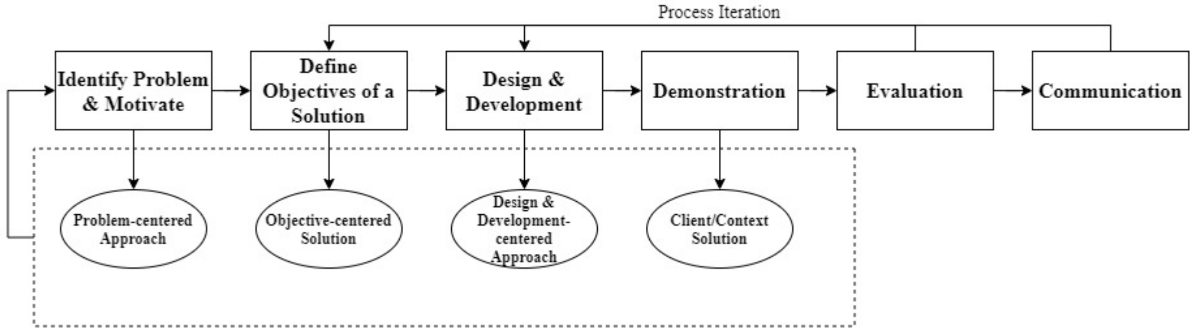

Process Iteration
Identify Problem & Motivate
Define Objectives of a Solution
Design & Development
Demonstration
Evaluation
Communication
Problem-centered Approach
Objective-centered Solution
Design & Development-centered Approach
Client/Context Solution

Figure 2.1: Visualisation of Design Science Research Method (DSRM) by Peffers et al. (2007)

The first activity defined as identifying problem & motivate, has been done in the first chapter of this research proposal. The problem is identified and a justification of why a solution would create value is given. In this way, the audience is motivated to continue reading and understand the reasoning behind the research. Resources required were knowledge of the state of the problem and of course the importance of the solution provided by the NVWA.

The second activity is done by desk research, i.e. literature review in combination with interviews. Existing solutions are analysed such that rational objectives are inferred from the specified problem, while being verified with primary data obtained from interviews. Knowledge with regards to the state of the problems and existing solutions is required and used for the construction and development of a design.

This leads to the core of the design science, which is designing and developing an artifact. This can be any designed object in which a research contribution is encapsulated in the design. The desired functionality, its architecture and the creation of the actual artifact is key here. This part can be found in Chapter 5 where the redesign is proposed and its motive of usage is illustrated by means of multiple use-cases.

After the redesign, the usefulness of the solution must be demonstrated and validated. This can for instance be done by means of a case study, experiment or an interview. In this case, for a qualitative research, an evaluative interview was chosen. The activity involves comparing the objectives of a solution to the actual observed results from use of the artifact in the demonstration phase. This can be a turning point for the researcher, leading to a possible iteration of the design process. If further improvement is desired, this is the point of action. If not, ergo the design is validated, the final design process is communicated to the relevant parties involved and a conclusion is drawn.

2.2. Approach

In order to answer the research questions established in Chapter 1, an extensive literature study in combination with interviews is conducted.

After an initial literature study, explorative interviews were performed to verify the open issues found and come up with a final knowledge gap. This concluded in the lack of transparency in the process, obstructing the increase in adoption. After this was clear, the main research question and sub-questions were constructed. A logical sequence was formed starting with the exploration of the current process of implementing drones by the NVWA. This was done in the same way as described before; by looking at secondary data (e.g. white papers) and informal meetings with the interviewees. The output of this sub-question led to the visualisation of the current work process including the identification of potential bottlenecks. This will be used as an input for the design phase, hence answering the main research question.

Then, the second sub-question is used to obtain a clear picture of how drone detecting services create value and to identify its barriers, referred to as disruptive threats. The creation of value has already been made clear during the introduction of drone detecting services. This was found by using secondary data and informal meetings of experts in the field. The list of disruptive threats or barriers is then used as an input for the design phase.

The third sub-question is concerning the sociotechnical effects of implementing and using drone detecting services by the NVWA. Here, first all stakeholders are identified and analysed in a social map. By means of constructive interviews, explained in the interview approach, the stakeholders' roles, motive and linkage with the NVWA are explained. Subsequently, a value map is constructed where the stakeholders' key values are described and potential value conflicts are analysed. By taking into account these values, the design can be made more responsible hence serves as an important input for the redesign phase.

Lastly, a redesign is proposed such that the bottlenecks found are mitigated while taking into account the key values of the stakeholders. A trade off of three different security techniques is performed based on a SWOT analysis and set criteria. As a solution, blockchain technology was found to perform best and is analysed in detail such that the benefits and motive of usage are clear. After, the implementation is illustrated by the construction of two use-cases in which the technology's most important characteristics are made clear. This is later evaluated by means of two evaluative interviews and a conclusion is drawn.

2.2.1. Desk Research Approach

Secondary data collection was done by means of an extensive literature review, i.e. desk research. By looking at the existing literature concerning drone detecting services and common issues concerning drones, a clear picture was given of the situation in the Netherlands. Desk research saves a lot of time which can effectively be spent in other data collection methods such as interviews. Furthermore, desk research allows easy gathering of data from different instances with similar cases, increasing the credibility of the research.

The search started by familiarising with IoT, UAS and its applications, by the use of search engines like Scopus and Sciencedirect. General papers were found by using key words such as ’IoT Development UAS’ and ’UAS Open Issues’. This led to an enormous amount of papers in various fields of research. By refining the search to the subject areas of Social Sciences and filtering on the number of citations from highest to lowest, only the most reliable papers were found. Skimming through the abstract and conclusions of the top papers was a good start for identifying the first papers and getting an initial idea of research.

After this, more analytical papers had to be found whereby the general IoT and drone development challenges are addressed by means of innovative approaches. Key words such as ’IoT Device Management’ and ’IoT Drone management’ were now used. Again, the search was refined by limiting it to the subject areas of Social Sciences and by filtering on the number of citations of the papers to acquire the most reliable sources. Similarities in content concerning the issues were found and used as a reference for informal meetings with the company. The issues were verified and access was granted to unpublished white papers and slides within the company. This helped refine the search to the scope of the Netherlands (and NVWA) and led to the identification of a knowledge gap.

The first two sub-questions were then answered using both scientific literature and media sources, in combination with explorative interviews. Besides, professional sources, or white papers, were used to help answer the sub-questions concerning the current state of drone detecting services, the value it creates and the negatives, referred to as disruptive threats, involved.

2.2.2. Interview Approach

For this research, multiple interviews were performed to obtain primary data of the analysed research questions. More specifically, semi-structured interviews were conducted to gain a better understanding of the information found in professional literature and to help find the hidden barriers in the process and implicit values of the stakeholders. A semi-structured approach was chosen such that the open questions are tailored to the interviewee and new topics were to be found. Besides, this explorative approach of conducting interviews was chosen such that a high level of information was obtained due to the interviewee being in the lead. Rough guidelines, as described below adapted from De Reuver (2019), were followed for constructing the interview questions.

- Use neutral wording (i.e. no biasing or leading questions);
- Avoid emotionally-loaded questions;

- Avoid ambiguous questions and words;
- Avoid twofold questions;

The first interviews were open and explorative, and performed on three types of experts within the NVWA to get an answer for the first subquestion. A general guideline was developed, ensuring the subjects of interest were discussed during the interviews. For the explorative mapping, as seen in Appendix A.1, three key subjects or phases were covered; a short introduction, obstruction mapping and ideas for improvement. In this way, together with the information found in secondary data, a valid view of the current obstacles and an initial idea for improvement was found.

Participants were chosen based on expertise and field of work. Informal conversations by phone and e-mail were held to get the best fitting candidates for the interviews. In this way, time was saved and high quality transcripts were obtained. All participants were found via the NVWA's contact base. An e-mail was sent out with a personal introduction, referral to the NVWA, introduction to the research and of course the reason of interest. Furthermore, a proposal for an online Teams meeting or phone call of +/- 30 minutes was given to reduce time wasted on planning a date and meeting physically. In most cases, this led to a fast and enthusiastic reply with a set meeting for the interview.
Initially, this led to three main interviewees; Head of the Team Remote Sensing & Data Acquisition (NVWA), Specialist Risk & Crisis Management / Strategic Advisor (External) and an AI specialist / Data Engineer (NVWA). As seen, two internal and one external employee was interviewed to get a clear first view of the problem. Note that the last interview questions differ a little from the first two interviews for further purposes in the research.

For the second stage, sub-question 3 answered in Chapter 4, interviews were conducted of all stakeholders involved in the implementation process of drone detecting services by the NVWA. The same procedure was taken whereby stakeholders were found via the NVWA's contact base. E-mails led to online Teams meetings whereby the following subjects were discussed; introduction to the organisation, linkage with the NVWA, organisation's values and obstructions to verify the results found in the first stage.

2.2.3. Interview Analysis

The conducted interviews were transcribed by means of notes and keywords taken during the interview. Note that due to confidentiality, the interviews were not recorded. For the sake of quality, the interviewee's wording and answers were quoted as literal as possible, such that no bias was created during the transcription and a realistic network could be formed. Transcripts of the interviews conducted can be found in Appendix A.1, A.2 & A.3.

After all interviews were conducted and transcribed, a qualitative analysis was performed. Since this research is both explorative and qualitative, qualitative analysis software was used to interconnect, manage and methodically analyse all text. Besides, the software, also known as ATLAS TI, allows to extract meaning and create visual structures from the data. Together with the secondary data, this will then serve as an input for the construction of a final framework.
The analyses was done based on a three-step coding approach, as seen in Figure 2.2. The first step consisted of ”Open Coding” which is where the researcher identifies the distinct concepts and themes for the categorisation of the transcript (Williams & Moser, 2019). Initial broad thematic domains such as ”Job Description” and ”Responsibilities” were made. This was classified by annotations and short explanations. The process of coding the interviews was done simultaneously such that logical codes were given and similar themes were found.

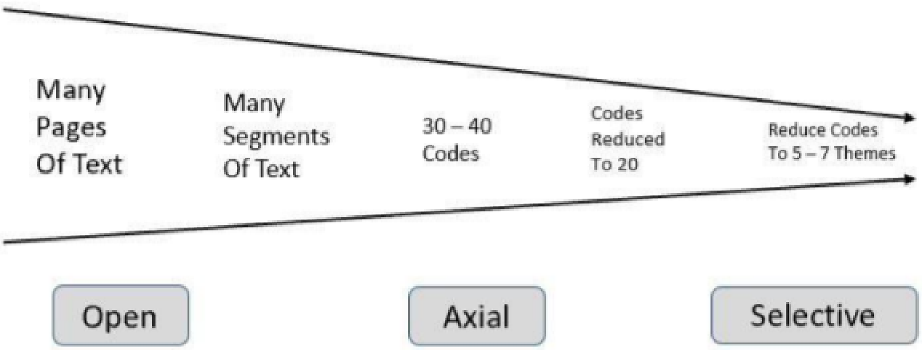


Figure 2.2: Schematic overview of the coding process; Open, Axial and Selective coding.

After this, the various codes were segmented and categorised more precisely. A comparison approach was taken whereby themes were created by comparing codes to similarly coded indicators in other interviews. According to Williams & Moser (2019), axial coding further refines and categorises the themes. The relationships between the codes can in this way be identified such that a clear image is obtained of the core codes.

The last step is referred to as selective coding and enables the selection and integration of the organised categories found during axial coding. This however leads to abstraction of the codes and necessary elaboration of the context. For this reason, selective coding has been done during the construction of the networks. The main codes found during axial coding were used and further explained. Moreover, main categories such as ”Linkage with NVWA” and ”Obstacles Drone Implementation” were selected and visualised in a network. In this way, a clear view of the relationships between the codes was obtained and the primary data could be qualitatively analysed. During selective coding, the thematic refining process led to a certain degree of causality or predictability. Visualising this in a network, ultimately led to meaning and the construction of a possible redesign. (Williams & Moser, 2019) Please note that the process of categorising, coding and analysing is done highly iterative.

2.3. Expected Deliverable

The deliverable for this research will be given in the form of a proposal for redesign of the current work process. More specifically, an enhanced process that can improve the responsible adoption of the technology is obtained. As seen in Figure 2.3, the output of every subsequent sub-question serves as an input for the redesign phase, ergo as an input for answering the main research question. The final redesign, which increases the responsibility and possibly the adoption rate of the technology, may benefit multiple parties in different contexts. Subsequently, revenue models or collaboration possibilities (e.g. a consortium) can be made possible by the use of the proposed technology in the redesign. A flow diagram of the research process and final outline can be found in Figure 2.3.

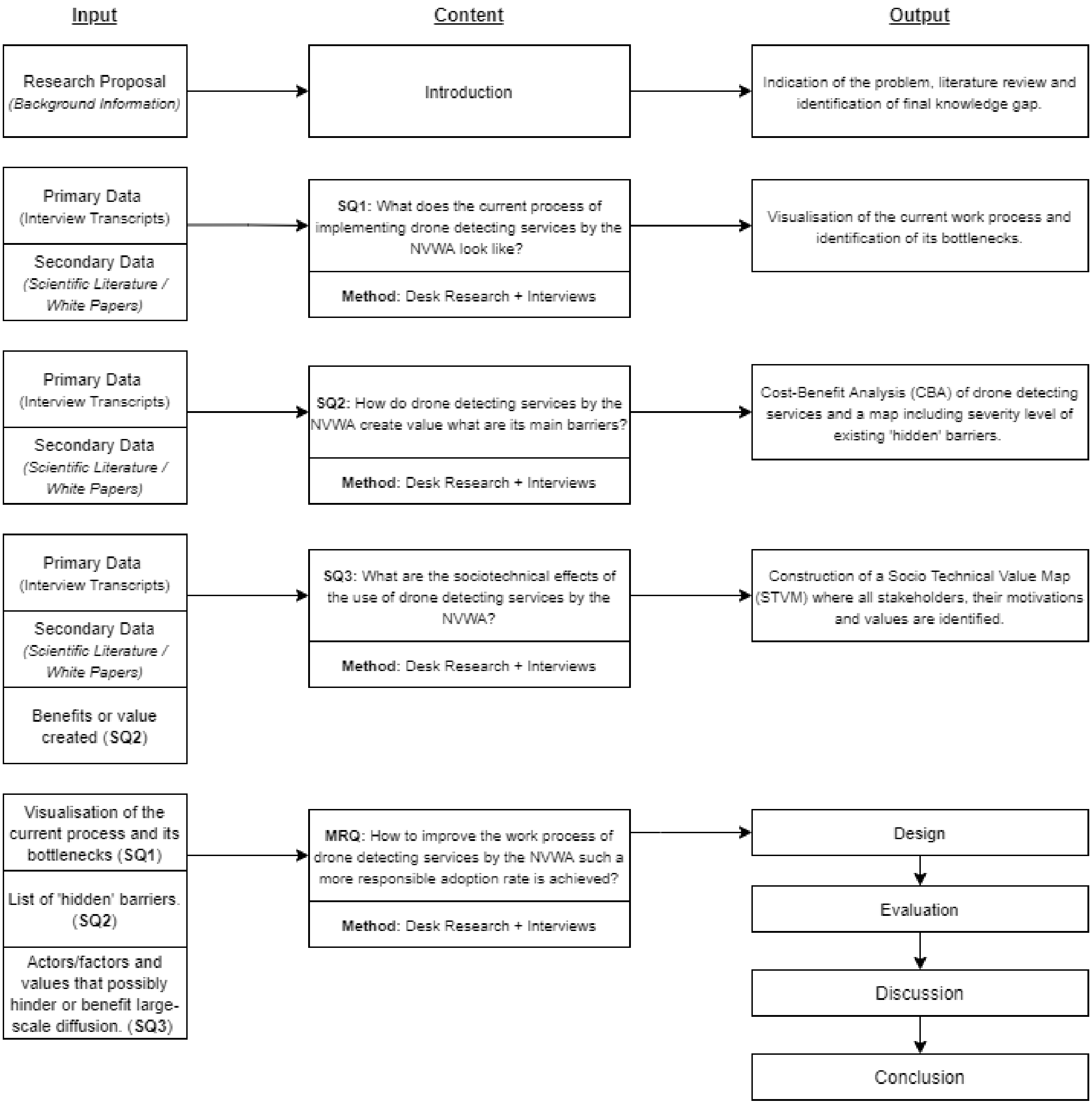

Input
Content
Output
Research Proposal (Background Information)
Introduction
Indication of the problem, literature review and identification of final knowledge gap.
Primary Data (Interview Transcripts)
Secondary Data (Scientific Literature / White Papers)
SQ1: What does the current process of implementing drone detecting services by the NVWA look like?
Method: Desk Research + Interviews
Visualisation of the current work process and identification of its bottlenecks.
Primary Data (Interview Transcripts)
Secondary Data (Scientific Literature / White Papers)
SQ2: How do drone detecting services by the NVWA create value what are its main barriers?
Method: Desk Research + Interviews
Cost-Benefit Analysis (CBA) of drone detecting services and a map including severity level of existing 'hidden' barriers.
Primary Data (Interview Transcripts)
Secondary Data (Scientific Literature / White Papers)
Benefits or value created (SQ2)
SQ3: What are the sociotechnical effects of the use of drone detecting services by the NVWA?
Method: Desk Research + Interviews
Construction of a Socio Technical Value Map (STVM) where all stakeholders, their motivations and values are identified.
Visualisation of the current process and its bottlenecks (SQ1)
List of 'hidden' barriers. (SQ2)
Actors/factors and values that possibly hinder or benefit large-scale diffusion. (SQ3)
MRQ: How to improve the work process of drone detecting services by the NVWA such a more responsible adoption rate is achieved?
Method: Desk Research + Interviews
Design
Evaluation
Discussion
Conclusion

Figure 2.3: Flow Diagram of the Research Process and Final Outline

3

Drone Detecting Services

To start off, the current state of drone detecting services implemented by the NVWA in the Netherlands will be analysed. This chapter is written to provide a literature basis about the definition of drone detecting services, the applications by the NVWA and to map the current work process. Besides, the overall added value and negatives caused by implementing drones in societal practices are described. This will help find the uncertainty factor among authorities and citizens, and could be used for connecting the found bottlenecks in the current work process. In this way, a clear map of the value it creates is given, which eventually can serve as an input to the main research question. The use of both scientific and professional literature will be used as to find an answer to the SQ1 and SQ2; "*What does the current process of implementing drone detecting services and sharing data in the Netherlands look like?*" and "*How do drone detecting services in the Netherlands create value and what are its main barriers?*", respectively.

Drone detecting services, also known as Drones as a Service (DaaS) (Choi, Sung, Park, Ahn, & Kim, 2017), have been expanding greatly in various application domains worldwide. The advent of drone utilisation in both public and civil domains has led to applications such as traffic monitoring and surveillance, parcel delivery, search and rescue missions (e.g. ER), remote sensing in agriculture and multiple other application domains (Valavanis & Vachtsevanos, 2015). Since this field of application is so broad and expanding greatly, the focus will be on the existing drone detecting services used by the NVWA in the Netherlands.

Custers, Oerlemans & Vergouw (2015), broadly analyse the current drone applications in the Netherlands and take into account both the opportunities and threats it imposes. A distinction is made between drones used in the private and public sector. Private being recreational while the public sector includes all drone applications executed by governmental institutions. Most judicial applications are in the field of prevention, detection and prosecution. More specifically, data is used for criminal enforcement and investigation (by the police department). Besides, it is also a tool for administrative law enforcement agencies. The NVWA is one of those agencies, with the end-goal to ensure food safety and animal welfare in the Netherlands. They do this by performing inspections, monitoring and enforcing activities. Their drone detecting services create value by being more efficient and safe in regular operations. The drone's agile characteristics, ease-of-use and accurate results has led to great results in various application domains. Below a list is given of some of the most prominent drone applications by the NVWA. For the sake of space, applications within the same domain are merged into one category. Please note that this could lead to some overlap between the activities mentioned.

- **Parcel-Scanning** - Drones are implemented to monitor and inspect large parcels such that a faster identification rate and more accurate results are obtained. Activities consist of determining the amount of cattle present, hence determining if a farmer follows the guidelines such that a grazing premium can be practised. Besides, the farmers can make use of the drone's capabilities to identify sick animals hence proactively take measures. This of course depends on the mission of the drone, i.e. which payload is included. Similarly, drones are used to identify (illegal dumped) cadavers for informing or enforcing purposes. By means of thermal sensors, the drone can easily identify a possible cadaver which normally takes hours to do by hand. (Custers et al., 2015)
- **Corrosion/Fracture Detection** - Another drone service performed by the NVWA consists of detecting corrosion on infrastructure. In October 2020 the NVWA, together with the Department of Waterways and Public Works, executed a project on the detection of corrosion in theme parks (de Graaff, 2020). In this context, the use of drones creates value due to its flexibility and accuracy, possibly leading to better preventative measures. The various imaging sensors allows the 2D and 3D mapping of the attractions, making preventative measures more reliable. Besides, thermal sensors allows the imaging of weld seams and possible weak points, e.g. fatigue or highly stressed joints. Apart from corrosion inspection in themeparks, the NVWA uses the same techniques to determine the vitality of trees surrounding the attractions. Possible fractures and weak points, which are normally hard or impossible to identify by eye, are identified by the drone's sensors such that preventative measures can be taken. (Custers et al., 2015)
- **Regulatory Enforcement** - Besides the parcel-scanning or inspection applications as mentioned before, the NVWA also experiments with enforcing nature legislation by performing operations along the coast or in nature reserves. More specifically, drones are implemented for the detection of illegal fisheries or fykes in the Netherlands (Custers et al., 2015). Usually this is done 'manually' by inspectors from a boat. This can however be labour-intensive and could lead to dangerous situations for the inspectors. Think about aggressive behaviour of trespassers or external factors such as bad weather conditions, e.g. a rough sea. Now, with the use of drones in combination with Artifical Intelligence, fykes can easily be identified and removed. The human interaction factor is removed which also increases the safety level. Enforcement is hence done in a more safe and effective way.
- **Safeguarding the Ecosystem** - The last category of activities consists of safeguarding the ecosystem, i.e. animal welfare and plant health. In 2018, the drones of the NVWA have proven to be successful in the detection of Asian Hornet nests (Natuur & Milieu, 2018). By means of triangulation and thermal sensors, large areas can be covered fast, making identification of a nest less labour-intensive. Besides, the drone can easily scan through densely wooded areas. The nest, which wasn't visible by the human eye, can now be identified by flying over the tree and looking at it from a different angle, i.e. bird's eye view. The same procedure has been proven to work for other species such as the longhorn beetle. The drones hence create value due to their effective identification rate and agile characteristics.

3.1. Payload Options

Payload is in this context defined as the mass the drone can transport, apart from its own components such as battery and structure. This is defined as the 'useful load' of the drone. For drones the payload is referring to all its attachments including the necessary electronics required, and carried, during an operation. It goes without saying that different services require different payload to fulfill their tasks. Moreover, different payload leads to different restrictions for operating. Since the payload options for drones are endless, only the most common used payload types used are covered. A distinction is made between the types of payload used in practice by governmental institutes such as the NVWA.

3.1.1. Sensors

The foremost type of payload used, consists of sensors. A sensor is simply a device capable of detecting or measuring a physical property. It can record, indicate or respond to this 'data'. Sensors used for drone operations however come in various forms. Most commonly used are cameras in combination with recording devices, e.g. microphones.

Most consumer drones are equipped with RGB cameras. In this way, the same RGB bands as the eye can be captured such that the images produced look almost exactly what one's eyes can see (Herrick, 2017). Other common used cameras in use by the NVWA are Near-Infrared (NIR) and Thermal Infrared (TIR) sensors. Both work with infrared light and can easily evaluate crop health and reveal the location and extent of discrete thermal inputs (Dugdale, Kelleher, Malcolm, Caldwell, & Hannah, 2019). All three make use of imagery and video data which is known to be privacy sensitive. (Cheung, Venkatesh, Paruchuri, Zhao, & Nguyen, 2009)

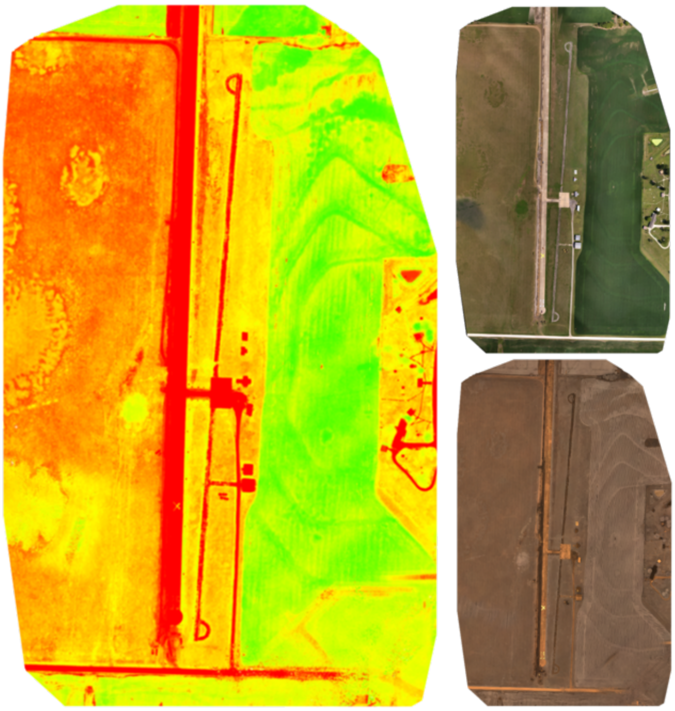


Figure 3.1: Example of a NDVI orthomosaic map (left) made from a combination of RGB (top right) and NIR (bottom right) imagery by Herrick (2017).

A Light Detection And Ranging of Laser Imaging Detection And Ranging (LiDAR) system, or sensor, sends out pulses of laser light and measures the exact time it takes for these pulses to return as they bounce from the ground (Customdrone, n.d.). It also measures the intensity of that reflection which allows easy 3D modelling and measurements at ground level. The 3D-mapping technique leads to the acquisition of 3D distance data to create models. Hence an anonymous picture of the area is obtained while protecting privacy. Solely in the case of unwanted/non-requested use of LiDAR, personal information about one's terrain could be obtained. This is however unlikely to happen in the analysed operations of the NVWA.

So-called chemical 'sniffers' are sensors that measure the chemical composition of substances. They are able to measure concentrations of small particles in the air such as fine dust, gases or vapors, but also substances in water or in the ground. The sensors exposed to the ambient air, continuously sniff the environment and give qualitative information about the air composition. Common applications range from detecting environmental crimes such as contaminated soil on farmland, to checking for toxic substances in the air due to factory emissions. (Custers et al., 2015) The implementation of drones with these sensors hence increases overall safety level of inspections. The data obtained, i.e. air composition, can be transferred to regulatory bodies and used for further notice. Possibly, the data contains privacy sensitive information.

The spectral information obtained from hyperspectral cameras attached to the drone, allows the collection and processing of spectrum information. In agricultural practices, more detailed crop and soil parameters can be retrieved, allowing the derivation of plant health information such as nutrient deficiencies, water stress and crop diseases (Migdall, Klug, Denis, & Bach, 2012). This information can be privacy sensitive, since one can analyse and monitor an individual's property.

With a rough limit of 1.5 meter depth, a Ground Penetrating Radar (GPR) enables to map through the surface of ground making surveillance operations more efficient. GPR works with electromagnetic waves that are sent into the ground via a transmitting antenna, which is reflected in a soil or construction when the material's properties change. The reflected waves are then recorded using a receiving antenna. Subsequently, the measurement data can be analysed for positioning and determining the depth and dimensions of objects and/or soil layers. The non-intrusive sensors can see through ice, rocks, freshwater, buildings or through structures at unsafe and hazardous environments. (T&A Survey, n.d.) Common practices such as detecting explosives can now be done by means of the drone sensor, hence increases safety level of such operations.

An Ultrasonic Sensor sends out a high-frequency sound pulse and then measures how long it takes for the echo of the sound to reflect back (Corrigan, 2020). The sensor consists of a transmitter and a receiver, and is mainly used by drones for object detection. Besides, the sensor is used in domains such as detecting flaws in structures. Lastly, meteorological instruments are often installed to measure phenomena such as wind speed, temperature and humidity. Again, the drone's agile characteristics in combination with these sensor enables measurements at unsafe and hazardous environments. (Custers et al., 2015)

A summary of the various payload options, required services and purposes of the NVWA is given in Table 3.1. As seen, many payload options can collect privacy-sensitive information, indicating the risk level of drone-use. This will be addressed upon in the next section.

Table 3.1: Various payload options, capabilities, added value, type of data and privacy-sensitivity

Type of Sensor	Capabilities	Added Value	Type of Data	Privacy-Sensitive
RGB	Produce realistic images using same RGB bands as human eye	- Realistic imagery - Fast field scouting	Imagery/Video	Possibly
NIR	Capture infrared light and thereby evaluate crop health	- Faster (crop health) detection rate	Imagery/Video	Possibly
TIR	Reveal the location and extent of discrete thermal inputs	- Temperature mapping	Imagery/Video	Possibly
LiDAR	3D-mapping; provide readings of the 'scanned' area and points on the ground	- Easy 3D modelling - Measurements at ground level	3D-models, terrain specifics	No
Chemical 'Sniffers'	Detect and recognize gases, vapors or odors	- Preventive tool	Air composition	Possibly
Hyperspectral Camera	Collect and process spectrum information	- Provide spectral information - More detailed (crop) detection	Imagery/ Hyperspectral	Possibly
GPR	Electromagnetic mapping of the subsurface in a non-intrusive way	- More efficient surveying - Increased safety level of soil investigations - Non-intrusive	Sub-surface information, schematic models	No
Sonar	Detecting and measuring distance between objects	- High accuracy - Also able to detect flaws in structures	Ultrasonic data	No
Meteorological Instruments	Measure phenomena such as wind speed, temperature and humidity	- More precise measurements	Meteorological data	No

Other Payload

This category consists of all other items, apart from its own components, the drone can transport and use for its operations. For simplicity, a distinction is made between four subcategories.

The first one consists of transporting purposes, ergo, transporting goods such as post packages, meals and medicines. The drones are in this context used for deliveries with urgent matters or to access unsafe and hazardous environments, e.g. supply of oil rigs. Besides, the drone can transport and 'drop' the payload for agricultural practices. More specifically, the drone can be implemented for fertilizing and spraying crops (NVWA, n.d.). The sensors mentioned above monitor and decide where to fertilise with great precision. In this way, solely the crops which require fertiliser are sprayed, saving both time and money. Hence the drone's agile characteristics enable more efficient handling and, in some cases, even increase the overall safety level.

Second, drones can be supplied with EHBO kits, AEDs or other first aid supplies required by emergency services. The drone's agile and high speed characteristics are highly favored in this field, hence add great value. Drones such as the Ambulance Drone, designed by the TU Delft in 2014 have shown great potential (Momont, 2014). Speeding up emergency response can prevent deaths and accelerate recovery dramatically. In cases such as heart failure, drowning, traumas and respiratory issues, a fast emergency response is crucial. The national implementation of drones supplied with lifesaving technologies such as an Automated External Defibrillator (AED), medication, Cardiopulmonary Resuscitation (CPR) hence adds great value and could potentially lead to more lives being saved.

Another subcategory consists of technical payload such as WiFi hotspots or jammers used for drone operations. Instances such as Facebook and Google have been planning and testing the implementation of solar-empowered internet drones since 2019 (Russel, 2019). Ultimately, this technology can be used for investigating and collecting data about an individual's position or internet behavior. The jammers on the other hand can serve as a tool to block communication between instances. This however hasn't been implemented yet in the Netherlands due to legal restrictions. (Custers et al., 2015)

The last two subcategories consist of payload used for advertising and military purposes. Advertising drones are mostly implemented during big events, e.g. in football stadiums or festivals. For the other subcategory drones can be supplied with military payload such as explosives and firearms. This has however not been implemented in the Netherlands yet. (Custers et al., 2015)

3.2. Disruptive Threats

Now as seen in Table 3.1, many payload options work with privacy-sensitive information which can potentially be seen as a threat. In this context, this is referred to as a disruptive threat due to the introduction of drones; a disruptive innovation.

According to Christensen, Raynor & McDonald (2013), a disruptive innovation is an innovation which stimulates a disruption towards current existing products, market and value network, while simultaneously replacing the previous technology. In this case, the drone is overriding current practices and technologies used in various application domains. The technology's promising characteristics has proven to be successful in multiple domains and is expected to grow even further as discussed in the trends in drone-use. It increases crop yields and its caused environmental advantages will result in a higher efficiency hence higher profit to be made. However, like any other disruptive innovation, the roll out and further implementation of the drone detecting services comes with a cost. Since the technology has been implemented various times, i.e. surpassed the the roll out stage, it is assumed that the benefits of using the observational technology outweigh its monetary costs. For this reason, cost is defined as the negative effects experienced by the surroundings and/or stakeholders. This will serve as measure of how valuable the technology is for the later defined stakeholders in this research.

3.2.1. Privacy, Safety & Security

The main issues of the digitisation era are associated to privacy, data protection and ethical issues. As described before and seen in Table 3.1, various payload options receive various types of data which might be privacy sensitive. Multiple factors such as the purpose of use, extent and type of information received by the drones, type of operator, location and of course the payload used, must be considered for mapping potential data protection and ethical impacts (Finn & Wright, 2016). A study by Finn, Wright & Friedewald (2013) compares UAS surveillance with CCTV and helicopter surveillance. They argue that with the use of surveillance-oriented drones, everyone is monitored regardless of whether their activities warrant suspicion. The absence of transparency and overt of drones, compared to CCTV, potentially impacts behaviour and action negatively. It is argued that individuals must assume they are constantly being monitored and hence must adjust their behavior accordingly; to protect themselves against the negative effects of intrusions. Furthermore, Fin et al. (2013) argue that UAS surveillance can undermine data protection principles such as transparency, consent and rights of access. Individuals might not even realise that they are subject to UAS surveillance at any given time.

In the Netherlands the privacy rights are enshrined in the Dutch Constitution and the European Convention on Human Rights (EVRM) (Custers et al., 2015). There exist specific provisions in the Code of Criminal Procedure for investigating and enforcing activities. Moreover, when personal data is collected and processed, the Dutch Personal Data Protection Act (WBP) applies and states that personal data may only be collected and processed if there exists a legal basis for it, while meeting set conditions. However, in the context of maintaining public order or in investigating criminal offences, governmental drones may be used if a clear trade off is made with other less intrusive measures, i.e. as a final resort. (Custers et al., 2015) This gives an indication of how the Dutch legal frameworks offer various legal guarantees for enhancing one's privacy.

It must however be noted that due to its increase in popularity and capabilities, the legislation concerning this innovation is constantly changing. In January 2021 the Dutch legislation concerning drones was adjusted to the EU regulations which requires a stricter registration and certification (de Jager, 2020). Moreover, the drone pilots must behave according the EU drone regulations, are categorised and must be registered by means of multiple certificates. Drones with a higher payload logically come with a higher risk level hence require more expertise and certificates. This is simply done to enhance one's safety and privacy level, and to reduce the risks.

Other security and safety concerns are related to the risk of collision with other manned aircraft, bystanders and their property, and animals due to malfunctioning or bad weather conditions (Filcak, Povazan, & Viaud, 2020). Especially drones with heavy or hazardous payload, operational in populated or protected areas, can do great damage. For instance in May 2021, a drone crash-landed on the nesting ground of elegant terns in Bolsa Chica Ecological Reserve in Huntington Beach California (Levenson, 2021). The drones interrupted the protected area, scaring off about 2,500 of the terns and leaving behind about 1,500 eggs. None of them were viable after they were abandoned and the drone operator is yet to be found. Also, think about the damage an in-air collision with other drones or aircraft can do. This clearly stresses the seriousness of the safety and security risks, drone detecting services imply. A lack of expertise or malfunction of the technology could seriously damage the environment such as the recent tragedy in California. One can only imagine what happens if a malfunction occurs in a populated area.

Lastly, security issues concerning the use of drones for maleficent purposes or data being exposed to adversaries must be addressed. In 2016, researcher Jonathan Andersson had shown how a specialized device called Icarus can be used to hijack and control widely-used hobbyist drones (Zorz, 2016). Icarus can discover the unique secret key shared between the drone and the operator's controller by observing its unsecured protocol. Then, by means of brute-forcing, the key is obtained and used to impersonate the operator's controller hence take over control. The drone hijacker can now act as its operator and exploit the drone's capabilities for its own (maleficent) purposes.

Subsequently, drones can be attached with potential damaging payload. Think about jammers or signal sniffing software, which can be used to explore the security of areas. Also the cameras attached, collect potential personal information which can be obtained by hackers. In 2016 a data leaking scandal was reported whereby the world's largest drone manufacturer (DJI) shared data with Chinese authorities (BBC, 2017). One must therefore be careful when using certain type of drones; the risk of data leakage, i.e. security threats, remains to exist.

3.2.2. Pollution

A last category concerning the negatives of drones has to do with pollution. A distinction is made between noise and visual pollution. A study by Christian & Cabell (2017), has found that the noise induced by drones is experienced to be more annoying to people than the noise by cars and trucks. The new technology appears to have a higher annoyance level in sound, i.e. higher noise pollution, due to its novelty and of course non-conventional sound. People are used to the sounds of cars and rely on them which makes them more willing to accept the noise (Christian & Cabell, 2017). Of course, one might argue this will change over the years when the drone's capabilities and acceptance level has increased significantly.

On the other hand, a study by (European Union Aviation Safety Agency (EASA), 2021) had shown that visual pollution is a serious concern indicated by respondents regarding delivery drones and air taxis. With the great expansion of application domains for drone detecting services, this might become a serious issue.

3.3. Current Work Process

After a brief literature study and review of the disruptive threats, the current work process of the NVWA must be visualised. It is chosen to divide the work process into three phases. The first phase is logically called 'Preparation' since it consists of all activities in preparation of the actual operation. The second phase is called 'Operation' which includes all activities performed during the actual operation. Lastly, a 'Processing' phase is distinguished which consists of all activities after the actual operation. Each phase is visualised in Figure 3.4 and further explained below.

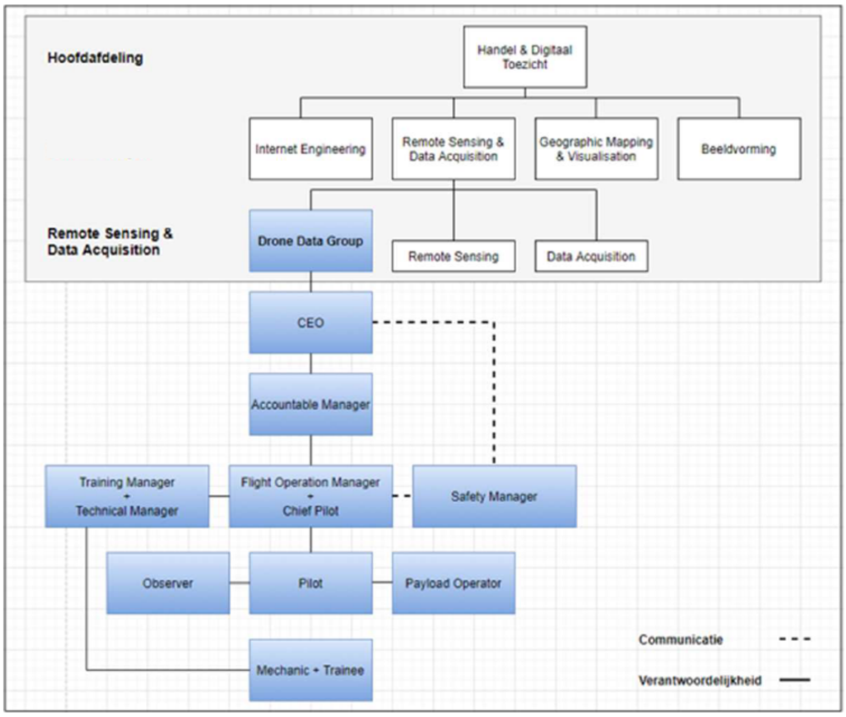


Figure 3.2: Positioning of the flight organisation (NVWA)

3.3.1. Preparation

The first phase consists of all activities in preparation for the actual operation; the drone detecting service. Subsequently, a distinction is made between area selection and drone selection. Please note that the selections are dependent on each other; the chosen area decides the suitability hence selection of drones available, and vice versa.

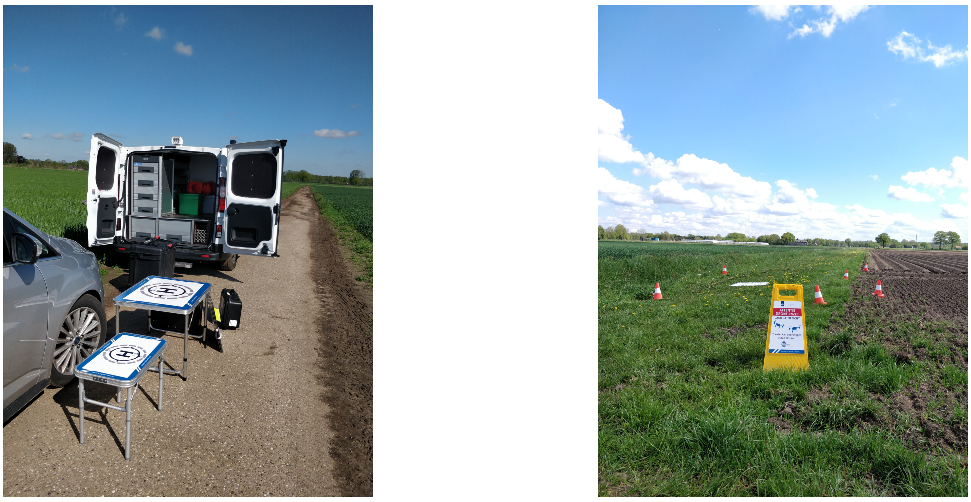
The first step of this phase is to digitally explore the location of interest. This is simply done by looking at secondary data available via satellites and fly maps. After an initial area mapping, the location of interest is physically explored. Possible obstructions and required permits are noted as an input for the drone- and payload selection. Logically, the next step is to determine all components and requirements for the operation. The selection of drones goes hand in hand with the selection of pilots and of course permits required. Depending on the operation, the corresponding roles of the operating team are chosen accordingly, as seen in Figure 3.2. The CEO is straightforwardly the responsible director of the team. The Accountable Manager (AM) and Flight Operation Manager (FOM) work hand-in-hand and check if all operations have been done safely, i.e. in accordance with the guidelines. The Training Manager (TM) is simply the manager present during a drone training. He/She provides the pilots in training with the required information and examines them. The Mechanic works remotely, i.e.

only if there are any technical issues with the equipment in-use. Then, for the actual operation, there is always a pilot and FOM present. The pilot is responsible for safely controlling the drone. Depending on the payload, a Payload Operator (PO) is chosen. The PO will control the payload equipped to the drone, e.g. LiDAR, and works simultaneously with the drone pilot. They must always be in direct contact during an operation. Observers are required for operations whereby the drone is used for large distances in possibly dangerous environments. The observer will be in direct contact with the pilot and warn if there are any hazards. Lastly, the Safety Manager (SM) is responsible for communicating direct hazards in the pilot's flight area. Think about informing the public and making sure the operating area is clear from obstacles et cetera.

After the team roles have been decided upon, the weather forecast is checked. Simultaneously, preparation in terms of safety management is required. Safety management is done for instance by determining the qualifications of the pilot and drone required, deciding upon weight category, depending on height and maximum payload of drone is required, and a preliminary risk analysis. For the risk analysis, both external as well as internal risks are taken into account. More specifically, external factors such as extreme weather conditions and internal factors such as technical or organisational issues must be considered. Mitigating measures are then taken beforehand. After all this is done, a final choice of equipment and transportation needed is made, such that the operation can start.

3.3.2. Operation

Next up, the operating phase as seen in Figure 3.4, is described in detail. In this phase, all activities performed during the actual operation, i.e. data collection by means of drones, are described. The first steps are iterative and performed to mitigate the impact of varying external factors, i.e. weather and environmental changes. More specifically, the weather is analysed and a final (physical) check of the area of interest is performed. After a green-light is given, the selected equipment must go through a safety check. This consists merely of checking if all payload is available, the drone application works properly, the SD cards are empty and to check if all batteries are fully charged. Besides, some preliminary safety measurements are taken in specific civil environments. Information regarding the drones of use is listed on a flyer and circulated in the area of interest. Also pawns and signs are defining the critical area as seen in Figure 3.3 (b).



(a) Transportation of the drones including required equipment.

(b) Safety measures taken in area of the operation.

Figure 3.3: Images of an actual drone operation performed by the NVWA

After this, a briefing of the flight crew will take place. Here all last minute changes, concerns and requirements with regards to the flight plan are discussed, as a final check. If everyone is okay with it and all permits are available, the actual operation can take place. Simple said, the drone and pilot can start collecting data for its specified purpose. Collecting data simply consists of using its payload, e.g. RGB or LiDAR, to get the desired information of the specified area. This data, e.g. imagery or video, is in most cases stored on the drone's internal SD card and transferred after the operation. There are developments in transferring this information real-time via a server, however hasn't been implemented yet. There remain to exist some restrictions related to GDPR which will be discussed later. This could however be another bottleneck of interest for improvement.

After the drone has collected all data and/or the SD card reached its maximum storage capacity, the operation phase has reached its end. The drone is landed on a safe platform and is stored safely in its case. The used SD card is taken out of the drone and also transferred to the office for the processing phase. Further wrapping up is done in the next phase.

3.3.3. Processing

The last step consists of all activities performed after the operating phase. This phase is referred to as the processing phase and discusses how the data is stored, transferred and analysed such that useful results are obtained.

After transferring data from the SD card to the office, the data can be analysed. According to P3 in Appendix A.3, this can only be done by a certain amount of computer instances with the required AI software of the NVWA. Based on its training sessions, the AI software used (e.g. PyTorch) translates the data by means of algorithms into useful results. First the imagery data is transferred to the AI processing pipeline on the device's cloudserver. This software analyses and transfers the data to the Geographic Information System GIS if it is marked as useful. If not, there is no point in analysing it further hence will be left unmarked. Additionally, the Point of Interest's coordinates and a recognition score of the detected object is transferred to the GIS map. The remote user, or inspector, can then use this data to localize, filter, export, share and complement objects with his/her own professional knowledge. (NVWA, 2021)
Simultaneously, personal data is removed and useful imagery data is 'stitched'. Image stitching is a specialised form of image mosaicing or merging, useful for modelling the 3D environment using panoramic images acquired from the real world (Chen, C.Y., & Klette, R., 1999). Image stitching methods treat the world as planar and simply stitch different images together by finding their relative positions. It is however known that the planar terrain assumption becomes invalid on farm grounds. According to Vasisht et al. (2017), obstructions such as uneven ground geometry, trees, animals or man-made structures observed in the video generates an unrealistic view, or parallax, which cannot be handled by the image registration algorithms that assume a planar scene. This is however assumed to be a minor issue since the model is merely used as a (rough) map for the inspector. Photogrammetry software such as Pix4D is used to organize, stitch and map the data collected within the NVWA. Besides it enables easy measurement of surface, distance and volume. This outputs an accurate and detailed quality report of the data and can be used for further inspection purposes.

The NVWA then uses GIS specialists to digitally enter, analyse and map the data. GIS is a framework used for gathering, managing, and analyzing data (Esri, n.d.). The software integrates many types of data and can spatially analyse a location and organize the layers of information into visualisations using maps and 3D scenes. Moreover, a better understanding is obtained including patterns, relationships and other insights such that smarter decisions are made. In this context, GIS mapping allows to draw accurate field borders and characteristics of for instance farmlands.

On the other hand, removing or blurring personal data is done manually and might be an interesting bottleneck to improve. According to P3 in Appendix A.1, the NVWA removes personal information manually; specific information such as faces of citizens and license plates are filtered out by manually going through the collected data and blurring or removing the personal information. According to P2 & P3, personal data collection is never the purpose of their operations hence occurs rarely. For this reason, the blurring process is kept plain and not the main focus of the organisation. For future applications and/or other organisations, this could however be an issue.

Going back to the process, after stitching, blurring and processing the data in the required software, the rough data is now transformed into useful data; a map or 3D model. The resulting data is visualized in a map which can easily be translated and used by the inspectors. The final step of the process hence consists of validating what is marked by the AI software. The remote user, or inspector, uses the data to localize, filter, export, share and complement objects with his/her own professional knowledge. The marked objects including its coordinates are directly analysed by the remote user, i.e. inspector. This risk-based analysis, or inspection, hence saves the remote user a lot of resources and time. A visualisation of the current work process and bottlenecks identified can be found in Figure 3.4.

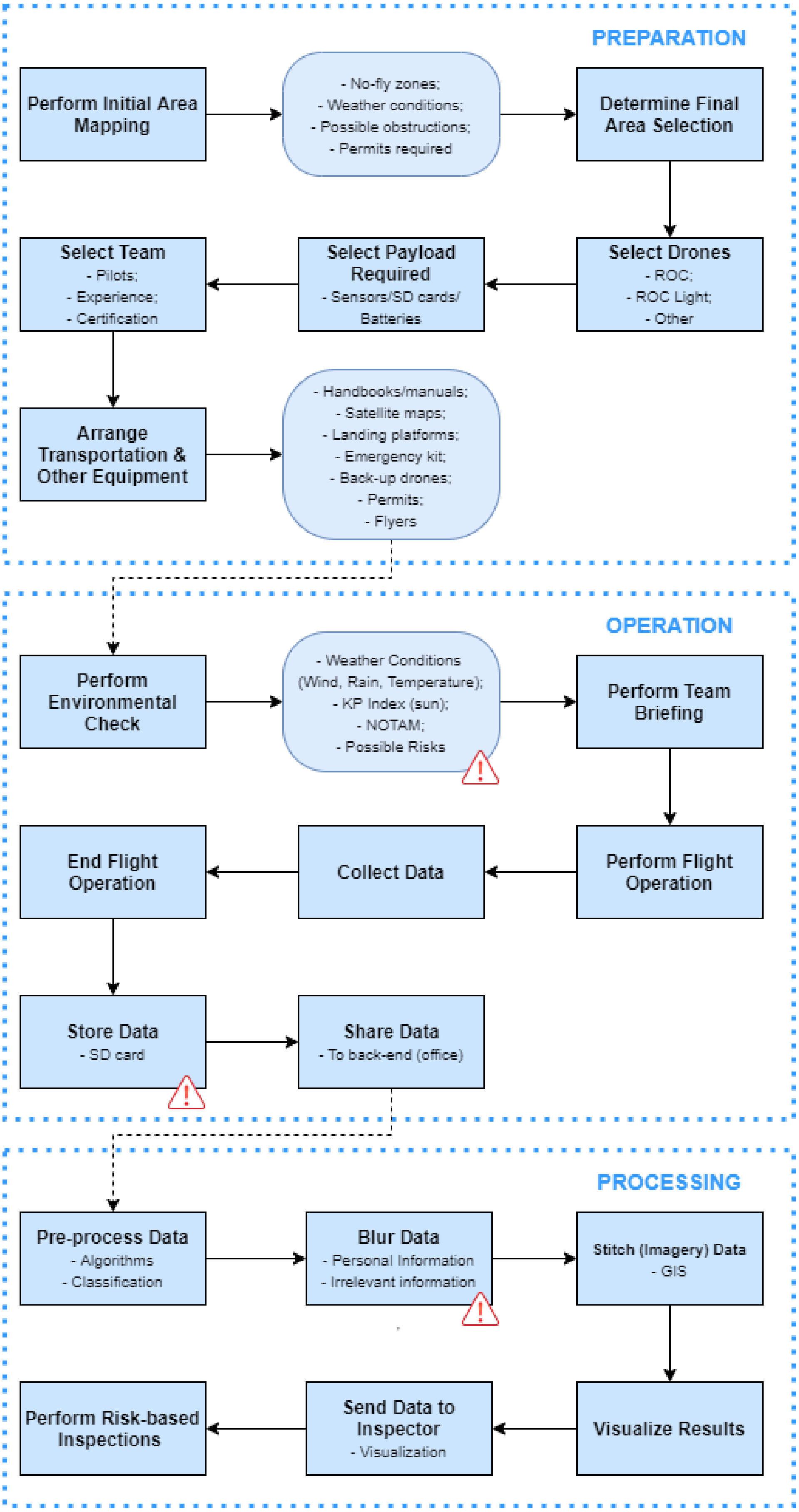


Figure 3.4: Visualisation of the current work process and vulnerabilities identified.

3.3.4. Bottlenecks Identified

Now to summarise, a few of the most prominent bottlenecks identified in the current work process are listed. This will be later used as a reference for the redesign phase. The bottlenecks identified consist of the following;

- **Blurring Techniques** - The organisation blurs data in the processing phase, after all data has been collected and stored on a hard drive. According to P3 in Appendix A.1, this process is done manually and can be inefficient and time-consuming. Besides, the process is not transparent hence formally cannot be validated by an authorised party. Although the NVWA hardly ever collects personal information, for future purposes and/or applications, this might be an issue and must be reconsidered.
- **Data Storage Techniques** - Similarly, after the collection of data by the drone, the SD card is removed and the data is transferred to the computer instance's hard drive. However, an SD card or hard drive's reliability or security level is known to be low. For that reason, it has been mentioned by multiple interviewees that a cloud server or different security technique is highly favored and being worked on. The governmental instances or authorities are however hesitant in using foreign services for the storage and sharing of potential personal information. For this reason, a cloud server has not been implemented yet and must be further analysed.
- **Safety & Security Protocol** - There is a need for transparency and a safety protocol in the process of implementing drones. Safety might be one of the most important values to be taken into account in the whole work process of implementing drone detecting services. For this reason, the preparation phase is so elaborate and consists of multiple checks and arrangements before the actual operation. Even just before an operation, multiple environmental checks are performed such as checking weather conditions, NOTAM and other external risks. This is done to ensure the operation is done in a safe way but also as a formality and tool to trace back in case an incident occurs. In practice, it has however been analysed that the checks consist of using multiple mobile applications with different interfaces and information. According to P3, this might be superfluous and could be done more simply by means of for instance one single application and a safety protocol. Of course those checks are crucial for a safe and responsible operation. Please note therefore that during this research, a privacy assessment is being worked on within the organisation. This includes taking proactive measures such as using social media, flyers and signs in the nearby environment to inform the public of the operation. Note however that in some cases, e.g. detection of illegal fisheries, this can unintentionally inform the trespassers hence make the operation useless. Nevertheless a well-structured and transparent safety protocol or privacy assessment is crucial to ensure the operation is done safe without affecting the nearby environment.

In Figure 3.5, some of the main obstacles identified by expert interviews in Appendix A.1 are shown. Please note that not all obstacles have been worked out in detail for the purpose of this research.

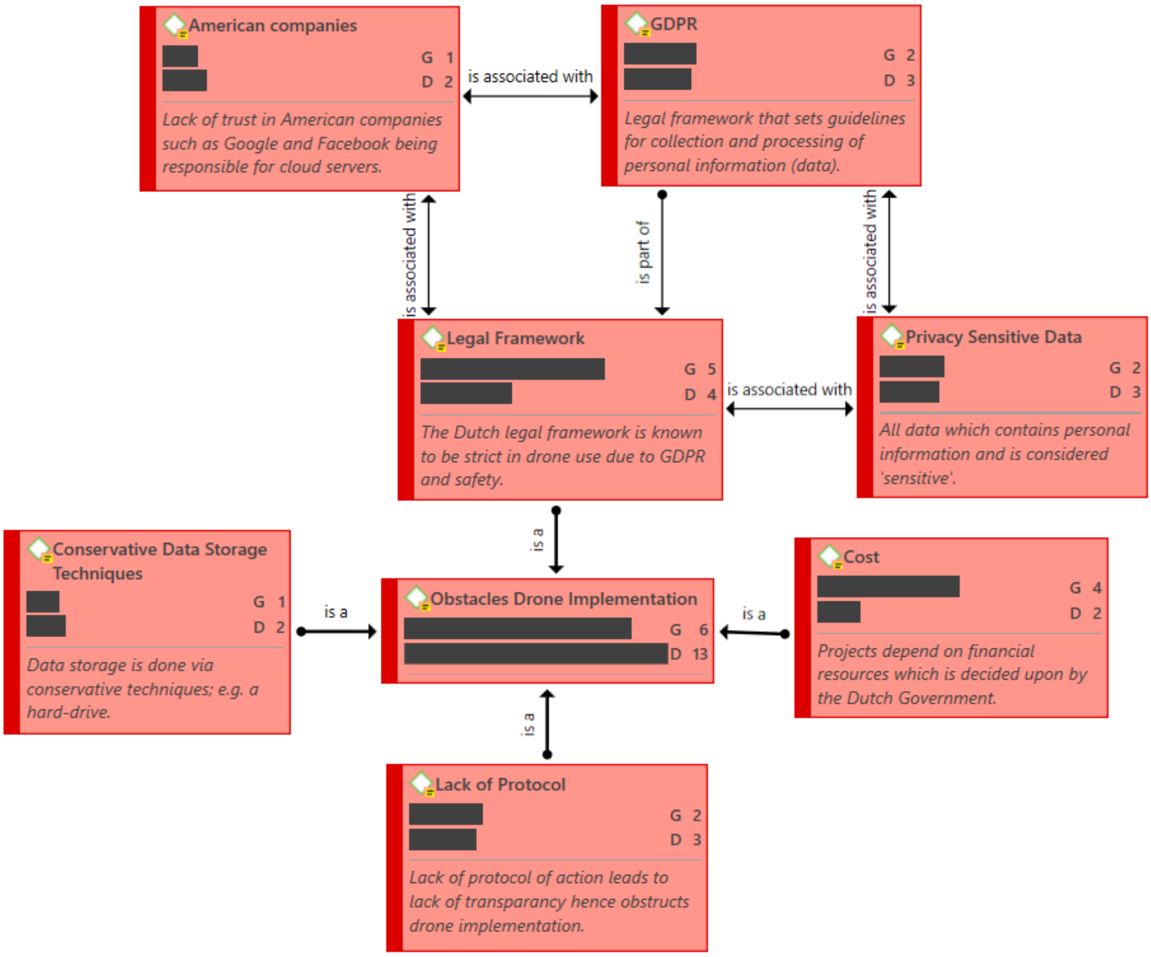
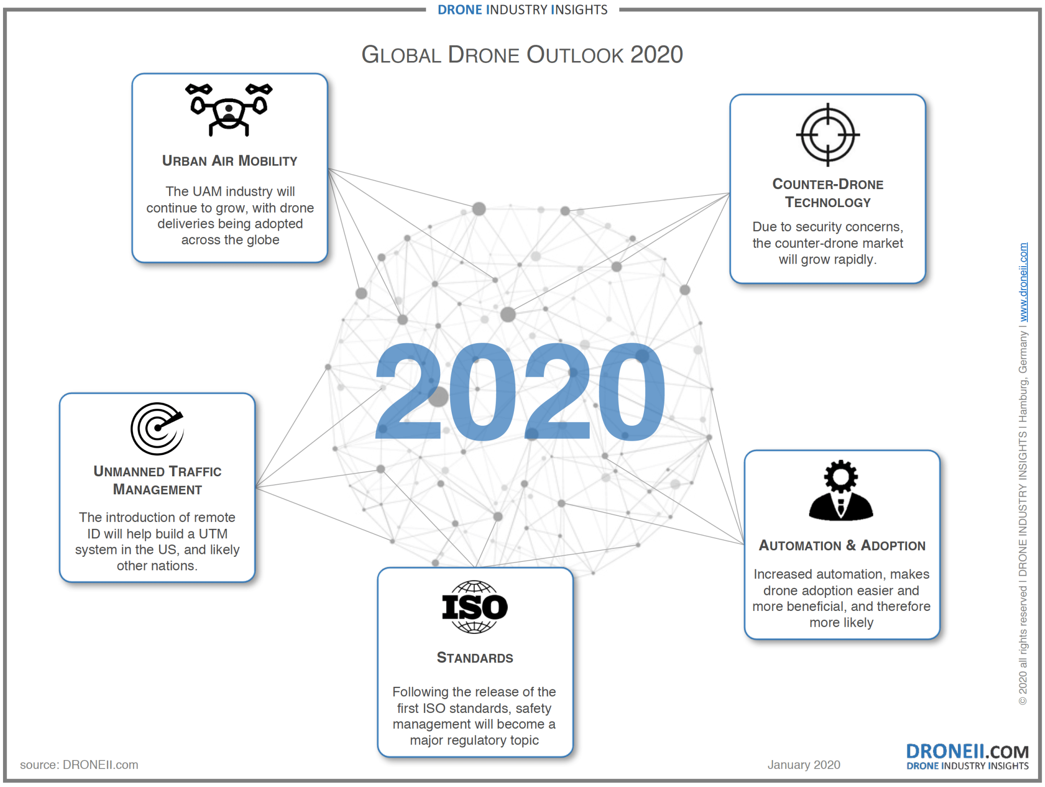

American companies
[redacted]
G 1
D 2
Lack of trust in American companies such as Google and Facebook being responsible for cloud servers.
is associated with
GDPR
[redacted]
G 2
D 3
Legal framework that sets guidelines for collection and processing of personal information (data).
is associated with
is part of
is associated with
Legal Framework
[redacted]
G 5
D 4
The Dutch legal framework is known to be strict in drone use due to GDPR and safety.
is associated with
Privacy Sensitive Data
[redacted]
G 2
D 3
All data which contains personal information and is considered 'sensitive'.
is a
Conservative Data Storage Techniques
[redacted]
G 1
D 2
Data storage is done via conservative techniques; e.g. a hard-drive.
is a
Obstacles Drone Implementation
[redacted]
G 6
D 13
is a
Cost
[redacted]
G 4
D 2
Projects depend on financial resources which is decided upon by the Dutch Government.
is a
Lack of Protocol
[redacted]
G 2
D 3
Lack of protocol of action leads to lack of transparancy hence obstructs drone implementation.

Figure 3.5: Obstacles identified by expert interviews from Appendix A.1

3.4. Trends in Drone-use

The commercial usage of drones is experiencing an increased acceptance level and many organisations start to adapt accordingly. According to (Insider Intelligence, 2021), the drone services market size is expected to grow from $4.4 billion in 2018 to $63.6 billion by 2025. The Association of Unmanned Vehicles Systems International (AUVSI) in the USA has predicted an economic impact of more than $80 billion between 2015-2025 with the agriculture accounting for 80% of the commercial market (Jenkins & Vasigh, 2013). Logically, this leads to more jobs hence greater economic wealth. As seen in Figure 3.6, Radovic (2020) distinguishes between five key trends in the year of 2020 for the commercial drone industry; Urban Air Mobility, Unmanned Traffic Management, ISO Standards, Automation & Adoption and Counter-drone Technology.

The first interesting trend discussed by Radovic (2020) has to do with counter-drone technology. Due to the increase in usage of drones (both commercial and recreational), an increasing in number of incidents has led to the growing of counter-drone technologies (Radovic, 2020). These will be mainly implemented by governmental actors and critical infrastructures such as airports and governmental buildings, to prevent incidents and security breaches.



DRONE INDUSTRY INSIGHTS

GLOBAL DRONE OUTLOOK 2020

URBAN AIR MOBILITY

The UAM industry will continue to grow, with drone deliveries being adopted across the globe

COUNTER-DRONE TECHNOLOGY

Due to security concerns, the counter-drone market will grow rapidly.

UNMANNED TRAFFIC MANAGEMENT

The introduction of remote ID will help build a UTM system in the US, and likely other nations.

AUTOMATION & ADOPTION

Increased automation, makes drone adoption easier and more beneficial, and therefore more likely

STANDARDS

Following the release of the first ISO standards, safety management will become a major regulatory topic

source: DRONEII.com

January 2020

DRONEII.COM DRONE INDUSTRY INSIGHTS

© 2020 all rights reserved I DRONE INDUSTRY INSIGHTS I Hamburg, Germany I www.droneii.com

Figure 3.6: Trends of commercial drone industry by Radovic (2020).

Another interesting trend to look at is Umanned Traffic Management (UTM). In 2020, the US Federal Aviation Authority (FAA) published guidelines for Remote ID and drone flights such that they can be identified on a distance. Remote Identification allows observers on the ground to track where an aircraft is flying and who is piloting it (Radovic, 2020).

In January 2021, the Dutch legislation concerning drones was adjusted to the EU standards (EASA) which requires stricter registration and certification. More specifically, every drone-operator has to be registered at the RDW and obtains his/her unique Remote ID. The pilot is then expected to make this code visual on all active drones. In this way, unmanned aircraft can be better managed as a preventive measure.

Simultaneously, safety management is an important trend which will continue over the years. Simple said, the increase in drone adoption and automation requires safety management to become a major regulatory topic. According to Radovic (2020), the key challenge in 2020 was the implementation and harmonization with national standard coordinating bodies and the compatibility of these with existing drone regulations. This trend is expected to increase simultaneously with the technology adoption.

Lastly, adoption and automation of drone detecting services is expected to increase significantly over the years. As described later on, various stakeholders are making use of the technology in varying application domains. This will mostlikely increase once the technology's robustness and its public acceptance is optimal.

4

Sociotechnical View

In this chapter, the use of drone detecting services for the NVWA's operations will be analysed in the point of view of a responsible innovation system. To do this, a sociotechnical approach is used whereby the technology dynamics including social factors are taken into account. More specifically, the Socio Technical Value Map (STVM) approach by Pesch & Werker (2019) is used. In this way, a clear map of all stakeholders, their motivations and values is obtained. Together with the visualisation of the current process and the identification of hidden barriers in Chapter 3, this chapter will help find an answer to the main research question. The use of scientific and professional literature in combination with interviews will help answer the final sub-question; *What are the sociotechnical effects of the use of drone detecting services in the Netherlands?*

Different social groups have different ideas and understandings of a new technology. Although this technology has passed its main developing stages, social values emerge and evolve during the development and implementation, hence must be analysed. According to Taebi, Correlje, Cuppen, Dignum & Pesch (2014), an ideal approach to responsible innovation requires interdisciplinary research that incorporates the ethics of technology, an institutional theory and policy planning. In this way, the role of values, an understanding of the roles of institutions realizing these values, and the stakeholder engagement, is understood and a responsible innovation is achieved. Von Schomberg (2013) defines responsible innovation as a framework that allows the satisfactory uptake of moral issues (public values) in technology development. According to Pesch & Werker (2019), there is an underlying idea that technology seems to be the straightforward application of scientific knowledge, labeled as a linear model of technology development. Pesch & Werker (2019) criticise this model and argue that technology and society can not be separated. ”Technologies are inevitably part of a sociotechnical system, which not only relates to the artefacts or objects that make up the technology, but also the use of these artefacts by concrete actors in specific societal contexts” (Pesch & Werker, 2019, p.22). Besides, technologies are build by people which have interests and motives for the process of innovation. As such, Pesch & Werker (2019) suggest the improvement of the model by developing a research framework that allows the identification of responsibilities that are connected to the emerging technology. This framework allows the identification of public values that are connected to (development) of the technology. This so-called Sociotechnical Value Map (STVM) informs about how the identified values can be actively taken into account in the further development of the sociotechnical system and plots the technology as part of a wider societal and institutional environment (Pesch & Werker, 2019).

4.1. Social Map

The first part of the Sociotechnical Value Map is called the Social Map. To correctly analyse the current system and the public values, its stakeholders must be found. According to Freeman (2015), stakeholders are defined as all individuals being affected by the roll out and use of the technology. As said before, to effectively develop the technology over the next couple of years, it is crucial to analyse the most prominent players and their corresponding interests and needs. For the purpose of this research, solely the stakeholders involved for the case in the Netherlands are being interviewed and discussed. More specifically, the stakeholders involved in the drone detecting services operated by the NVWA are discussed. See Appendix A.2 Stakeholder Interviews for the full interview transcripts. Please note that the NVWA's interests and values are not discussed here since this has been done before. A legend including colour codes used for the data analysis can be found below.

Stakeholders
Obstacles
Linkage with NVWA
Values

Figure 4.1: Legend of colour codes used for Stakeholders (Blue), Obstacles (Red), Linkage with NVWA (Yellow) and Values (Green).

A final list of all stakeholders interviewed including the interviewee's profession, instance and purpose can be found in the table below. Please note that this table also includes actors which have been interviewed for the previous chapters.

Table 4.1: List of interviewees including profession, instance and purpose for interview

Profession	Instance	Relevancy
Specialist Risk & Crisis Management / Strategic Advisor	NVWA (External)	Explorative
Specialist Remote Sensing & Data Acquisition / Senior Inspector	NVWA	Explorative
AI Specialist / Data Engineer	NVWA	Explorative
Lector Advanced Forensic Technology	Saxion	Stakeholders
Technical/Accountable Manager (Aerosensing dept.)	ILT	Stakeholders
Accountable Manager (Drone Team)	Rijkswaterstaat	Stakeholders
Operational Specialist Dutch Police Department	Dutch Police Dept.	Stakeholders
Owner Metal Recycling & Barrel Rental	'Outsider'	Stakeholders

4.1.1. Dutch Government

The Dutch Government, i.e. Dutch Ministries, can be seen as a main player in the development and implementation of drone-use in the Netherlands. They are mainly responsible for regulating and of course funding the technology, e.g. R&D. In the Netherlands, the Ministry of Infrastructure and Water Management Human Environment has three sections; policy, implementation and inspection (Rijksoverheid, n.d.-b). Subsequently, different agencies are responsible for the three sections. These will be further discussed as separate stakeholders later on. Now, the Dutch Government's interest is mostly to enhance the law, i.e. safe and sustainable living environment. Subsequently, enhancing an individual's privacy rights, i.e. security, is an important value. The national implementation of drones is approved, provided that no personal data is saved. Only under certain strict conditions, personal data may be saved. Ethical aspects such as safety, privacy, non-discrimination and freedom must be taken into account. For this reason, the technology must be proven to be safe, secure and reliable. This goes hand in hand with the value reputation. Whenever a governmental drone causes an accident, the Dutch Government must take responsibility and experiences critics of external parties. This simultaneously causes reputation damage which is of course not favored nor increases the adoption rate. The external parties' trust is of great importance to the Dutch Government hence must be preserved. More specifically, risks related to the values safety and security are mitigated greatly. Nevertheless, according to the interviewees from ILT and Rijkswaterstaat, the Dutch Ministry is eager to innovate when the benefits and process is clearly illustrated. A schematic view of the Dutch Government's values adapted from the interviews and secondary data is provided in Figure 4.2. The Dutch government has both a high interest and power level on the development of drone detecting services in the Netherlands. After all, they provide the financial resources for the existence and expansion of the instances and their drone teams.

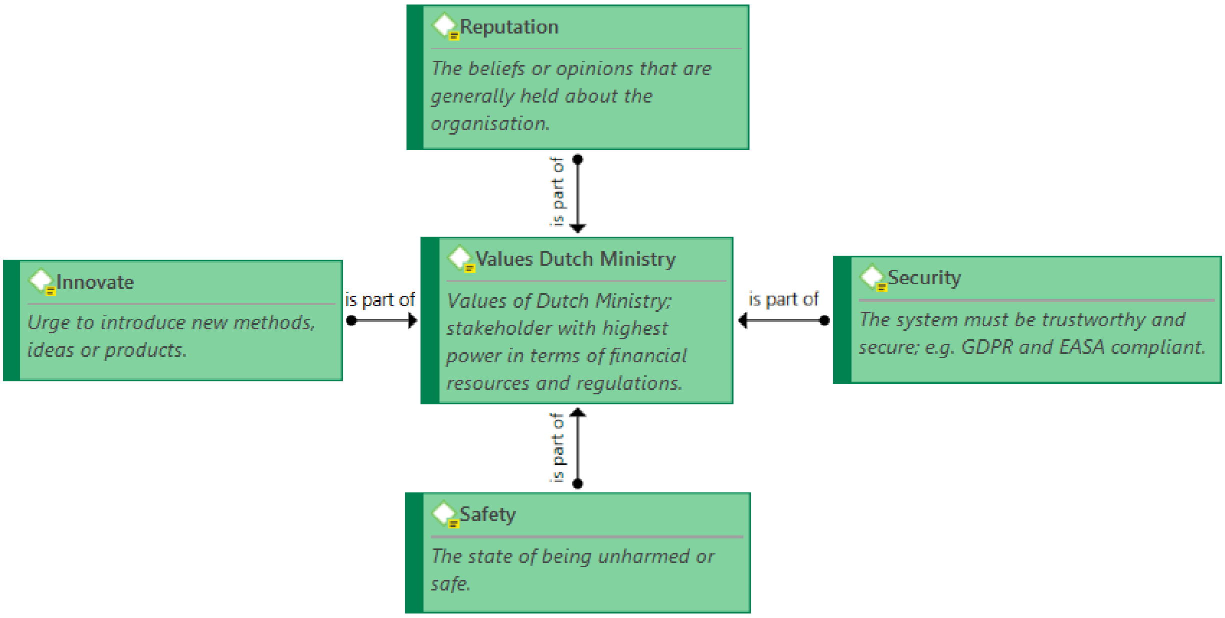

Reputation
The beliefs or opinions that are generally held about the organisation.
is part of
Innovate
Urge to introduce new methods, ideas or products.
is part of
Values Dutch Ministry
Values of Dutch Ministry; stakeholder with highest power in terms of financial resources and regulations.
is part of
Security
The system must be trustworthy and secure; e.g. GDPR and EASA compliant.
is part of
Safety
The state of being unharmed or safe.

Figure 4.2: Schematic view of the Dutch Government's values, adapted from secondary data and interviews in Appendix A.2

4.1.2. Human Environment and Transport Inspectorate (ILT)

In the policy section, the agency called Human Environment and Transport Inspectorate (ILT) oversees compliance with statutory regulations by private individuals and companies (Rijksoverheid, n.d.-b). More specifically, ILT strives for safety and sustainability among the aviation, within the Dutch borders. Subsequently, ILT regulates the commercial airlines, recreational and sports aviation, training institutions and flight simulators (Rijksoverheid, n.d.-a). According to S2 Appendix A.2, ILT is mainly involved in preparing and supervising tasks.

Relating ILT to the NVWA's drone activities; ILT makes sure permits are requested, no-flight zones are enhanced and is responsible for all other enforcing activities with the end goal of a safe and sustainable living environment. Besides, S2 mentions they are mutually responsible for the pilot training, certificates and permits required.

ILT's values however differ from the Dutch Ministry. According to S2, there seems to be a higher motive for innovation in his team, compared to higher up; the board of directors and Ministry. There exists a high dependency on ”budget and trustworthiness”; obstacles which make expansion difficult.

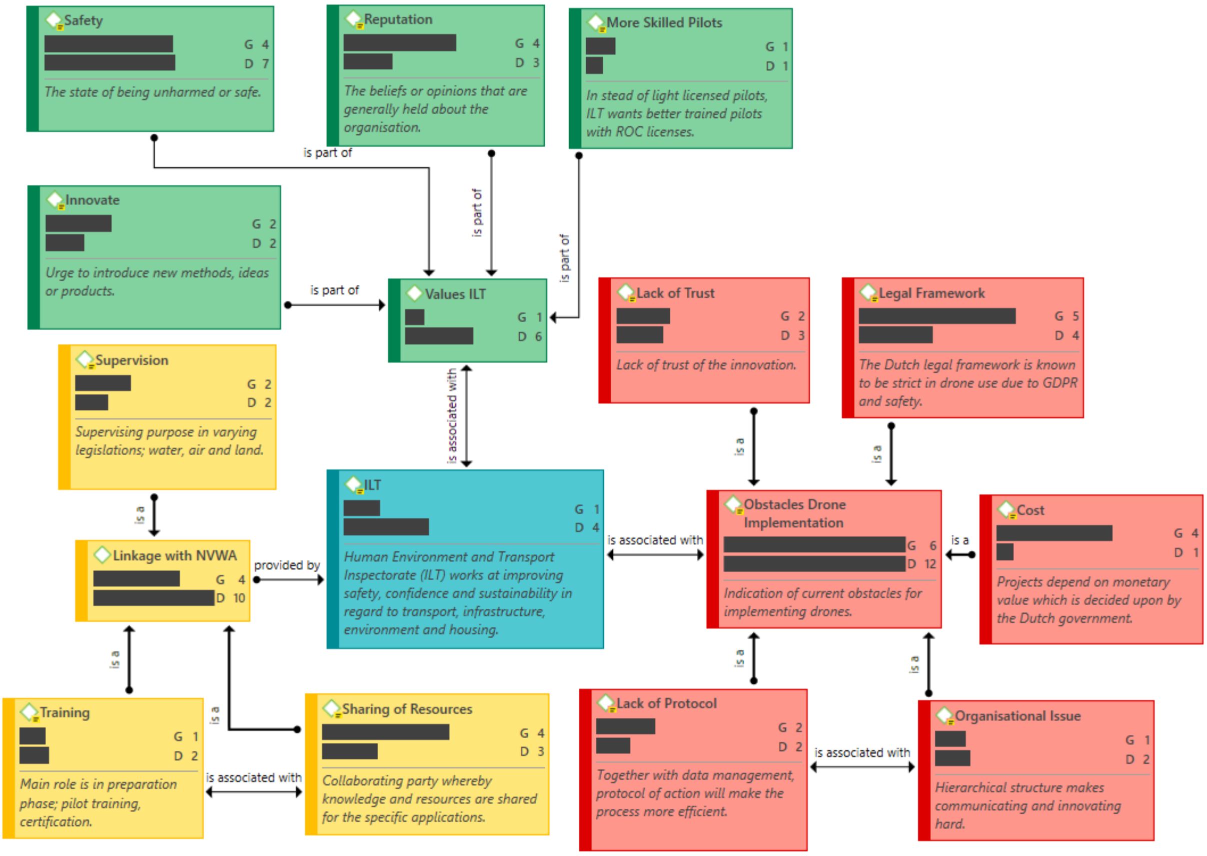

Safety
[redacted]
G 4
D 7
The state of being unharmed or safe.
Reputation
[redacted]
G 4
D 3
The beliefs or opinions that are generally held about the organisation.
More Skilled Pilots
[redacted]
G 1
D 1
In stead of light licensed pilots, ILT wants better trained pilots with ROC licenses.
is part of
is part of
is part of
is part of
Innovate
[redacted]
G 2
D 2
Urge to introduce new methods, ideas or products.
Values ILT
[redacted]
G 1
D 6
Lack of Trust
[redacted]
G 2
D 3
Lack of trust of the innovation.
Legal Framework
[redacted]
G 5
D 4
The Dutch legal framework is known to be strict in drone use due to GDPR and safety.
Supervision
[redacted]
G 2
D 2
Supervising purpose in varying legislations; water, air and land.
is associated with
is a
is a
is a
ILT
[redacted]
G 1
D 4
Human Environment and Transport Inspectorate (ILT) works at improving safety, confidence and sustainability in regard to transport, infrastructure, environment and housing.
Linkage with NVWA
[redacted]
G 4
D 10
provided by
is associated with
Obstacles Drone Implementation
[redacted]
G 6
D 12
Indication of current obstacles for implementing drones.
is a
Cost
[redacted]
G 4
D 1
Projects depend on monetary value which is decided upon by the Dutch government.
is a
is a
is a
is a
Training
[redacted]
G 1
D 2
Main role is in preparation phase; pilot training, certification.
is associated with
Sharing of Resources
[redacted]
G 4
D 3
Collaborating party whereby knowledge and resources are shared for the specific applications.
Lack of Protocol
[redacted]
G 2
D 2
Together with data management, protocol of action will make the process more efficient.
is associated with
Organisational Issue
[redacted]
G 1
D 2
Hierarchical structure makes communicating and innovating hard.

Figure 4.3: Schematic view of ILT's responsibilities linked to the NVWA, values and experienced obstacles for expansion, adapted from interviews in Appendix A.2

Finally, ILT values safety as the most important factor. Since they carry such a huge responsibility, and must safeguard their reputation as inspection service, they value safety more than all other.

4.1.3. Rijkswaterstaat

The Rijkswaterstaat is an executive agency that ensures the policy set by the Ministry is implemented. Note that this agency is responsible for the design, construction, management and maintenance of the main infrastructure facilities in the Netherlands (Rijksoverheid, n.d.-b). As described in Chapter 3, most current drone detecting services are not implemented in coastal environments. For this reason, the Rijkswaterstaat is not always an important stakeholder in the current operations.

However, as been found in the Interviews in Appendix A.2 and seen in Figure 4.4, the Rijkswaterstaat has two perspectives where they connect with the NVWA; 'Advising role' and 'Sharing of Resources'. Respectively, their big IT service and available resources makes them the 'more experienced party' hence acts as an advising role for the NVWA. They are responsible for setting the base, e.g. for the training of both the NVWA and ILT, and obtain more experienced and skilled pilots. They share their knowledge, and in some cases, their drones among each other for the sake of efficiency. More specifically, whenever an operation takes place and is interesting for both parties, they are allowed to perform flights for each other and share the collected data (except for personal information). This must however be planned and stated beforehand in the flight plan.

Their values are similar as ILT's values; again safety has the highest priority in terms of incident control

& prevention. Besides, their reputation as an executive agency for the government makes safety value even more. In case a drone fails, induces a risky situation or even causes environmental damage, the resulting reputation damage can be critical. As S3 stated, public acceptance remains an issue hence whenever a drone causes damage and gets negative media attention, the consequences for the Dutch drone teams will be fatal. According to S3, all parties will suffer whenever this happens and it will take years to gain back the trust of the civilians and the governmental directors in charge.

In terms of power, Rijkswaterstaat has a relatively high power since they are one of the pioneers in using drone detecting services in the Netherlands. Their leading-edge technologies, experience and knowledge makes them one of the leaders. However, please note again that the Dutch Ministry is in charge for the financial resources hence their possibilities for expansion.

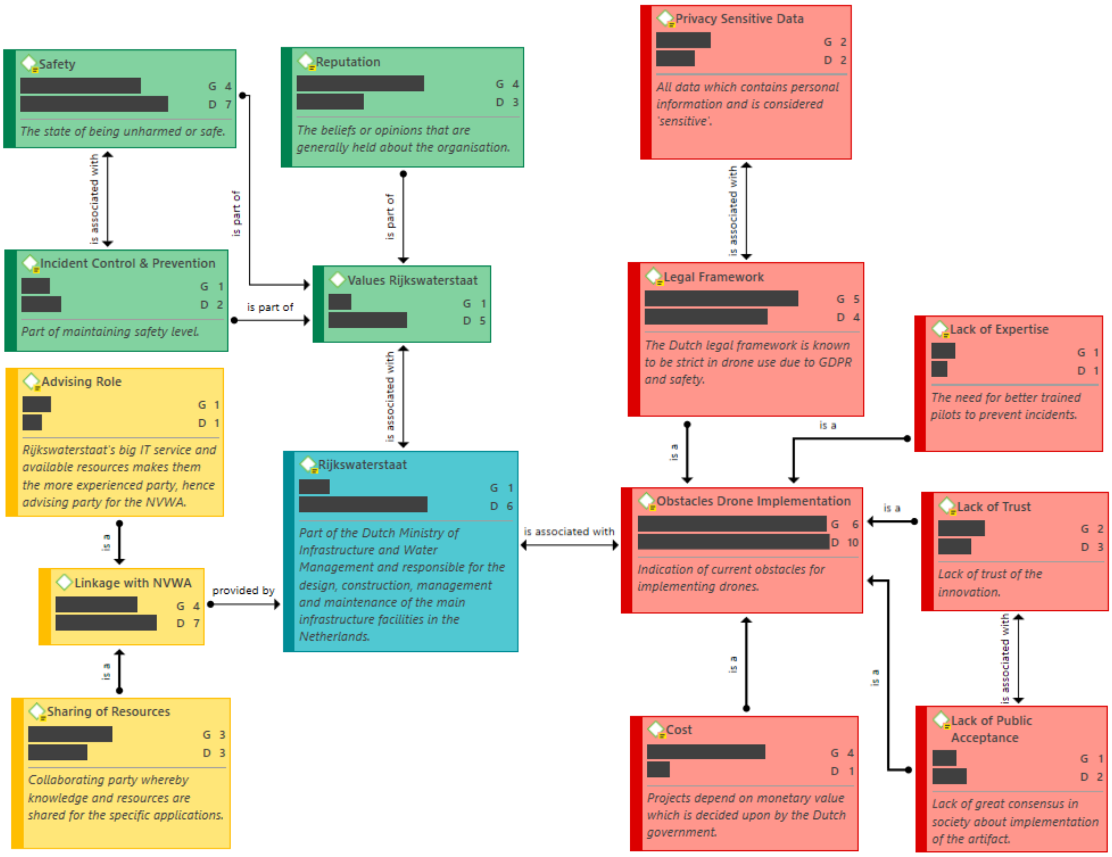

Safety
[redacted]
G 4
D 7
The state of being unharmed or safe.
Reputation
[redacted]
G 4
D 3
The beliefs or opinions that are generally held about the organisation.
Privacy Sensitive Data
[redacted]
G 2
D 2
All data which contains personal information and is considered 'sensitive'.
is associated with
is part of
is part of
is associated with
Incident Control & Prevention
[redacted]
G 1
D 2
Part of maintaining safety level.
is part of
Values Rijkswaterstaat
[redacted]
G 1
D 5
Legal Framework
[redacted]
G 5
D 4
The Dutch legal framework is known to be strict in drone use due to GDPR and safety.
Lack of Expertise
[redacted]
G 1
D 1
The need for better trained pilots to prevent incidents.
Advising Role
[redacted]
G 1
D 1
Rijkswaterstaat's big IT service and available resources makes them the more experienced party, hence advising party for the NVWA.
is associated with
is a
is a
Rijkswaterstaat
[redacted]
G 1
D 6
Part of the Dutch Ministry of Infrastructure and Water Management and responsible for the design, construction, management and maintenance of the main infrastructure facilities in the Netherlands.
is associated with
Obstacles Drone Implementation
[redacted]
G 6
D 10
Indication of current obstacles for implementing drones.
is a
Lack of Trust
[redacted]
G 2
D 3
Lack of trust of the innovation.
is a
Linkage with NVWA
[redacted]
G 4
D 7
provided by
is a
is a
is associated with
Sharing of Resources
[redacted]
G 3
D 3
Collaborating party whereby knowledge and resources are shared for the specific applications.
Cost
[redacted]
G 4
D 1
Projects depend on monetary value which is decided upon by the Dutch government.
Lack of Public Acceptance
[redacted]
G 1
D 2
Lack of great consensus in society about implementation of the artifact.

Figure 4.4: Schematic view of Rijkswaterstaat's responsibilities linked to the NVWA, values and experienced obstacles for expansion, adapted from interviews in Appendix A.2

4.1.4. Knowledge Institutions

Knowledge institutions are defined as universities, laboratories, and all other institutes providing valuable knowledge regarding the technology. In this case, universities and institutes responsible for the insight of value creating innovations concerning the drone detecting services in the domain of the NVWA are distinguished.

Currently, there are two main knowledge institutions currently working hand-in-hand with the NVWA on improvements and innovative insights; Hogeschool Saxion and Wageningen University & Research. Together with instances such as the Police, ILT, Rijkswaterstaat and the NVWA, they perform experiments and test new sensors to make the service more effective and analyse other potential application domains. S1, lector advanced forensic technology, works closely with the Dutch Police Department and mentions four lines of research; Nanoforensics, Forensic Robotics, Data Science & Crime, and lastly, Silent Witness & Coldcase. The first two are of particular interest since this coincides with the Dutch Police's activities with forensic drones, as mentioned by S4 in Appendix A.2. Saxion's motives such as ”faster detection rate” and ”lower level of human interaction” closely coincide with the need to innovate as seen in Figure 4.5. It must however be noted that ”safety” remains an important value in this process. This is due to the fact that governmental instances will make use of the technology hence cannot afford accidents.

Besides the linkage ”sharing of resources”, S4 mentions that Saxion and the police are, together with the other instances mentioned, working on the construction of a consortium whereby the use of resources is shared among each other such that faster results can be booked. This project called Drone2Go has the aim to form a collaboration between 5 Dutch first responding teams (ILT, NVWA, Dutch Police Department, Fire Department and Rijkswaterstaat) to explore the potential of autonomous drone by stimulating these technologies.

It can hence be concluded Saxion has high interest in the technology. However in terms of power, Saxion relies due the safety factor and financial resources, on other parties such as the Dutch Government. Also, there are some restrictions in the lines of research, as mentioned by S4. This clearly shows a difference in power with regards to the other stakeholders mentioned. An overview of Saxion's responsibilities linked to the NVWA, its values and its experienced obstacles for expansion adapted from the Interviews in Appendix A.2, can be found in Figure 4.5.

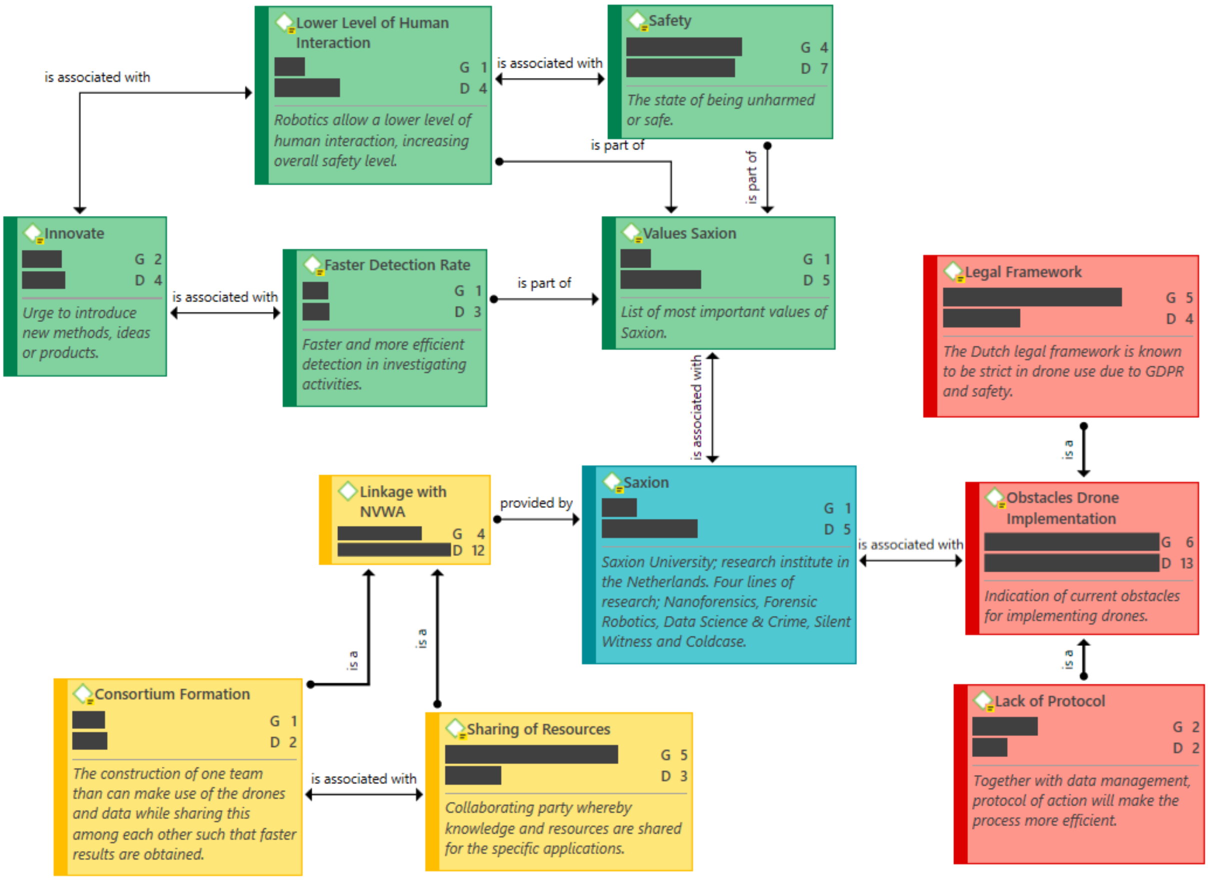
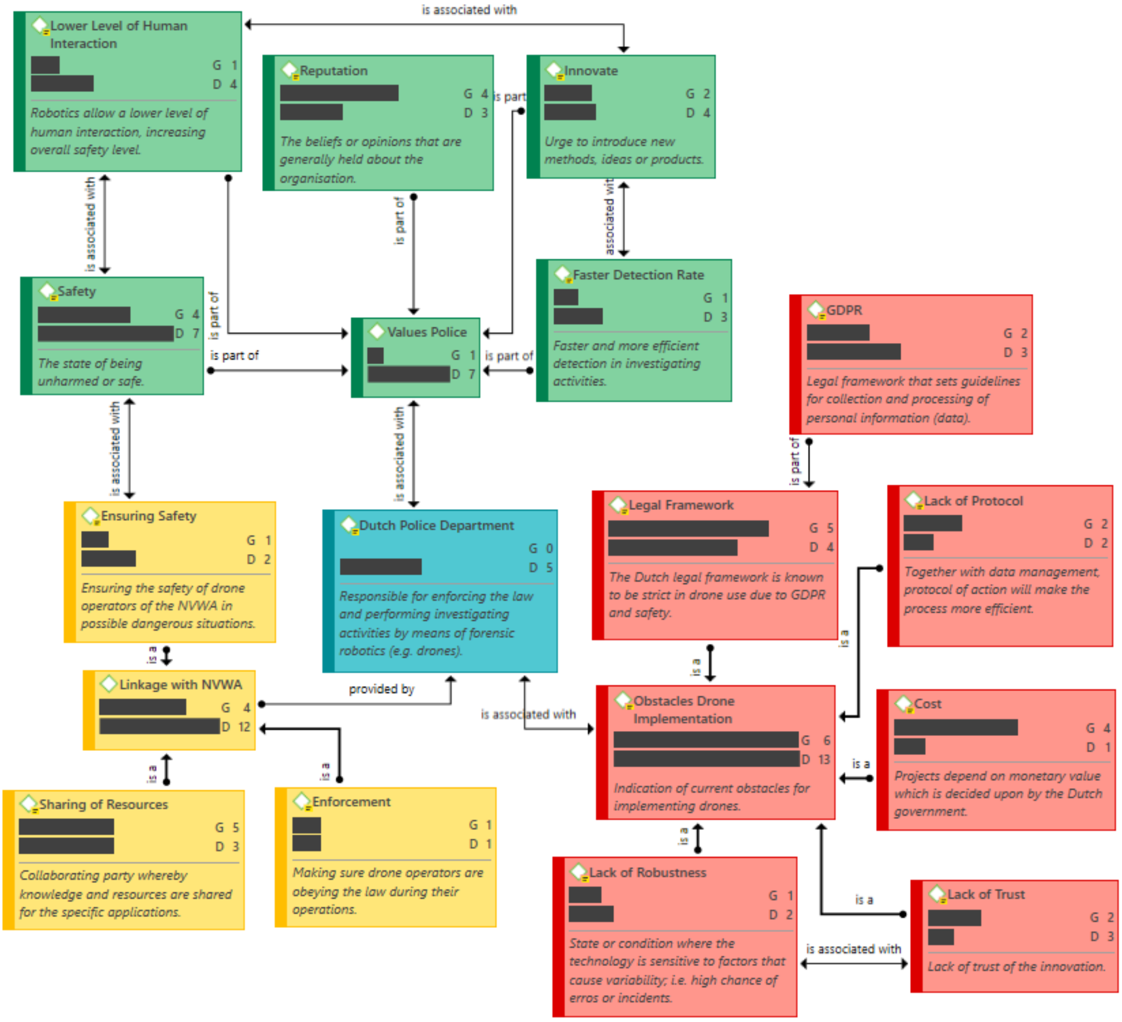

Lower Level of Human Interaction
[redacted] G 1 D 4
Robotics allow a lower level of human interaction, increasing overall safety level.
Safety
[redacted] G 4 D 7
The state of being unharmed or safe.
Innovate
[redacted] G 2 D 4
Urge to introduce new methods, ideas or products.
Faster Detection Rate
[redacted] G 1 D 3
Faster and more efficient detection in investigating activities.
Values Saxion
[redacted] G 1 D 5
List of most important values of Saxion.
Legal Framework
[redacted] G 5 D 4
The Dutch legal framework is known to be strict in drone use due to GDPR and safety.
Linkage with NVWA
[redacted] G 4 D 12
Saxion
[redacted] G 1 D 5
Saxion University; research institute in the Netherlands. Four lines of research; Nanoforensics, Forensic Robotics, Data Science & Crime, Silent Witness and Coldcase.
Obstacles Drone Implementation
[redacted] G 6 D 13
Indication of current obstacles for implementing drones.
Consortium Formation
[redacted] G 1 D 2
The construction of one team than can make use of the drones and data while sharing this among each other such that faster results are obtained.
Sharing of Resources
[redacted] G 5 D 3
Collaborating party whereby knowledge and resources are shared for the specific applications.
Lack of Protocol
[redacted] G 2 D 2
Together with data management, protocol of action will make the process more efficient.
is associated with
is associated with
is part of
is part of
is associated with
is part of
is associated with
provided by
is associated with
is a
is a
is a
is a
is associated with

Figure 4.5: Schematic view of Saxion's responsibilities linked to the NVWA, values and experienced obstacles for expansion, adapted from interviews in Appendix A.2

4.1.5. Dutch Police Department

The Dutch Police Department is yet another player involved in the process of implementing drone detecting services. Straightforwardly speaking, they are responsible for enforcing the law. The Netherlands is known for its strict legal framework concerning aviation hence must be enforced. The police often comes into play to check if the right safety measures are taken and the right permits and certificates are present. Furthermore, in addition to the country-specific regulations of the Netherlands, the NVWA must follow the drone regulations put in place by the European Union Aviation Safety Agency (EASA). The Police department in combination with governmental agencies such as ILT make sure to supervise and enforce where necessary. Moreover, the Dutch Police Department has a safety ensuring role for the NVWA. Meaning that whenever a dangerous situation arises for the NVWA, e.g. angry landowners or bystanders, the police comes into play and safeguards the NVWA's equipment and team.

According to S1 & S4 lector advanced forensic technology at Saxion and the Dutch Police Department in Appendix A.2, the police is working on improving forensic technologies by looking at forensic robotics and nanoforensics. More specifically, experiments are performed whereby the drone detecting services of the NVWA are being adapted to the police's operations. S1 mentions the use of sniffer drones for the identification of narcotics and cadaver-identifying drones for the identification of human bodies, also referred to as ”hidden graves”. By sharing knowledge and resources, faster and more efficient results can be booked in investigating activities. Besides, the use of robotics allows a lower level of human interaction hence increases overall safety level. As mentioned before when describing Saxion's values, their ultimate goal is to form a consortium with all first responding teams such that the drones and data can be shared, and faster results are obtained. There hence exists a great interest in the technology with a relatively high power. Legally speaking, the police has a higher power to use drone detecting services and collect data than most other parties described before. A summarising network view including the Police's responsibilities, experienced obstacles and values adapted from the conducted interviews, can be found in Figure 4.6.



Lower Level of Human Interaction
G 1
D 4
Robotics allow a lower level of human interaction, increasing overall safety level.
is associated with
Reputation
G 4
D 3
The beliefs or opinions that are generally held about the organisation.
is part of
Innovate
G 2
D 4
Urge to introduce new methods, ideas or products.
is associated with
is part of
Safety
G 4
D 7
The state of being unharmed or safe.
is part of
is part of
Values Police
G 1
D 7
is part of
Faster Detection Rate
G 1
D 3
Faster and more efficient detection in investigating activities.
GDPR
G 2
D 3
Legal framework that sets guidelines for collection and processing of personal information (data).
is associated with
is associated with
is part of
Ensuring Safety
G 1
D 2
Ensuring the safety of drone operators of the NVWA in possible dangerous situations.
Dutch Police Department
G 0
D 5
Responsible for enforcing the law and performing investigating activities by means of forensic robotics (e.g. drones).
Legal Framework
G 5
D 4
The Dutch legal framework is known to be strict in drone use due to GDPR and safety.
Lack of Protocol
G 2
D 2
Together with data management, protocol of action will make the process more efficient.
is a
is a
is a
Linkage with NVWA
G 4
D 12
provided by
is associated with
Obstacles Drone Implementation
G 6
D 13
Indication of current obstacles for implementing drones.
is a
Cost
G 4
D 1
Projects depend on monetary value which is decided upon by the Dutch government.
is a
is a
is a
Sharing of Resources
G 5
D 3
Collaborating party whereby knowledge and resources are shared for the specific applications.
Enforcement
G 1
D 1
Making sure drone operators are obeying the law during their operations.
Lack of Robustness
G 1
D 2
State or condition where the technology is sensitive to factors that cause variability; i.e. high chance of erros or incidents.
is a
is associated with
Lack of Trust
G 2
D 3
Lack of trust of the innovation.

Figure 4.6: Schematic view of Dutch Police's responsibilities linked to the NVWA, values and experienced obstacles for expansion, adapted from interviews in Appendix A.2

4.1.6. Outsiders

The last group of stakeholders are the external stakeholders and defined by all individuals affected by the roll out and use of the technology in their environment. This group is categorised as 'outsiders' in this stakeholder analysis. As a rough guideline, an interview was performed with an individual that owns a company on private property. To draw an accurate picture of its values and interests, the interview in combination with secondary data such as the media and newspapers, are used. For the interview, a different approach was taken such that valid results were obtained. The questions asked were more directive such that a clear picture of the individual's interests, values and existing obstacles was drawn.

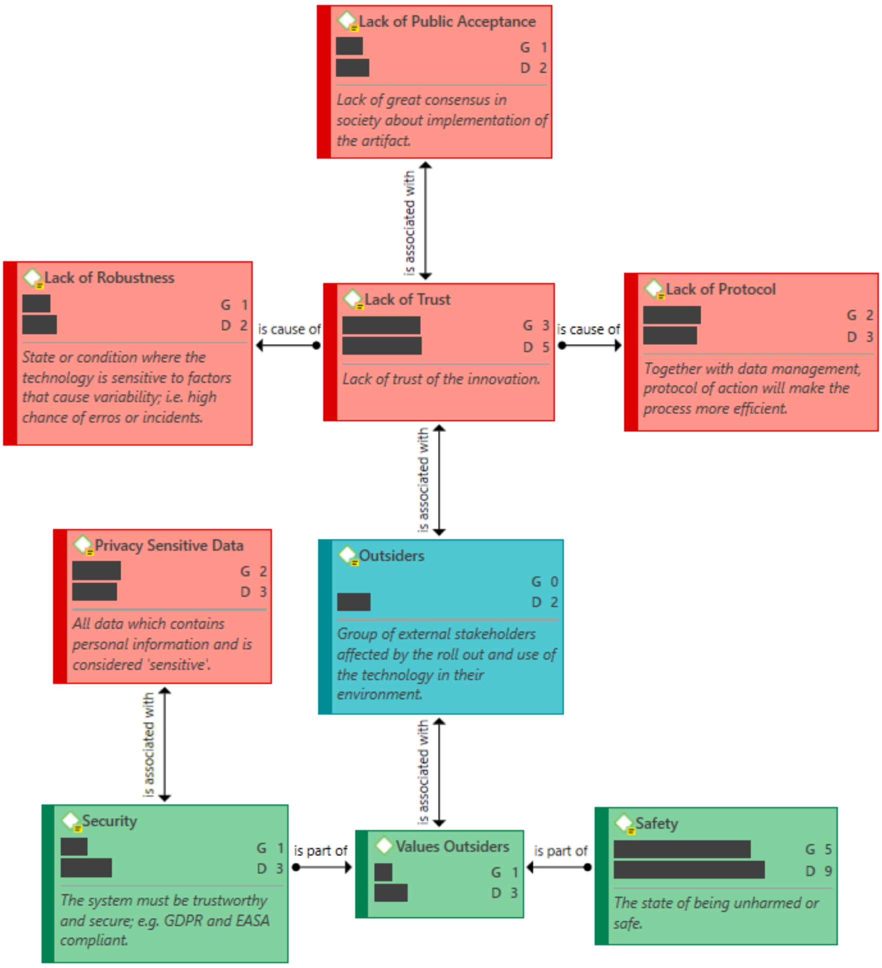

Lack of Public Acceptance
[redacted]
G 1
D 2
Lack of great consensus in society about implementation of the artifact.
is associated with
Lack of Robustness
[redacted]
G 1
D 2
State or condition where the technology is sensitive to factors that cause variability; i.e. high chance of erros or incidents.
is cause of
Lack of Trust
[redacted]
G 3
D 5
Lack of trust of the innovation.
is cause of
Lack of Protocol
[redacted]
G 2
D 3
Together with data management, protocol of action will make the process more efficient.
is associated with
Privacy Sensitive Data
[redacted]
G 2
D 3
All data which contains personal information and is considered 'sensitive'.
Outsiders
G 0
[redacted]
D 2
Group of external stakeholders affected by the roll out and use of the technology in their environment.
is associated with
is associated with
Security
[redacted]
G 1
D 3
The system must be trustworthy and secure; e.g. GDPR and EASA compliant.
is part of
Values Outsiders
[redacted]
G 1
D 3
is part of
Safety
[redacted]
G 5
D 9
The state of being unharmed or safe.

Figure 4.7: Schematic view of Outsiders' values adapted from secondary data and interviews in Appendix A.2

The outsider interviewed has a company with private property in the Netherlands and experiences inspections on a regular basis, i.e. inspect environmental and working conditions. As shown in Figure 4.7, the interviewee has mentioned two main values of interest; safety and security. It was indicated by S5 there is a lack of trust in the technology. Moreover, the interviewee lacks transparency in the process which questions the security of the technology, hence data collected. Personal information is highly valuable to this group of stakeholders hence must be protected by all means. Also the safety level in terms of property or personnel damage was mentioned and should be taken care of. This coincides with the open issues found in existing literature.

In terms of power/interest, this group of stakeholders has a medium interest and a high power level. The interest level is found to be relatively medium due to other parties having higher interest in innovating and expanding. This stakeholder's interest is purely based on enhancing safety and security, which is of high importance to any other stakeholder. The power level is found to be high due to the fast influence of (social) media nowadays. As stated by multiple interviewees, reputation is an important factor to be taken into account. The governmental agencies have a high responsibility and should be careful with their operations. One inexperienced pilot can cause a huge damage to the drone technology's, hence Dutch Government's, reputation. As S3 mentions in Appendix A.2; 'If one of our drones unintentionally collects and shares privacy sensitive information or in the extreme case crashes into someone's house, public acceptance will be damaged heavily'. The consequences can even be empowered by (social) media and causes huge reputation damage. Think about the various conspiracy theories brought up by 'regular civilians' on social media about 5G. Their lack of trust in the Dutch Government is empowered by negative (social) media attention and leads to delays and difficulties in the further roll out of the technology. In the case of 5G, this had led to fear, various protests and even vandalism to transmission towers (Spieksma & Voss, 2020).

This stresses the importance of trust and reputation of the Dutch Government. For this reason, the outsiders or civilians are given a relatively high power level. Although the Dutch Government is responsible for the regulations concerning privacy and safety, as proven in the past, the average Dutch civilian can cause big damage to the further roll out of the technology.

4.1.7. Power - Interest Matrix

For the sake of completion of this analysis, a clear overview of all power and interest levels of the involved players is visualised in a Power-Interest Matrix.(Poplawska, Labib, Reed, & Ishizaka, 2015) As was mentioned before and noticeable in Figure 4.8, currently the Dutch government has the highest power over the development and implementation of drone technologies in the analysed research. Their interest level is medium while most others experience a high level of interest. Furthermore, only the knowledge institutions experience a low level of power.

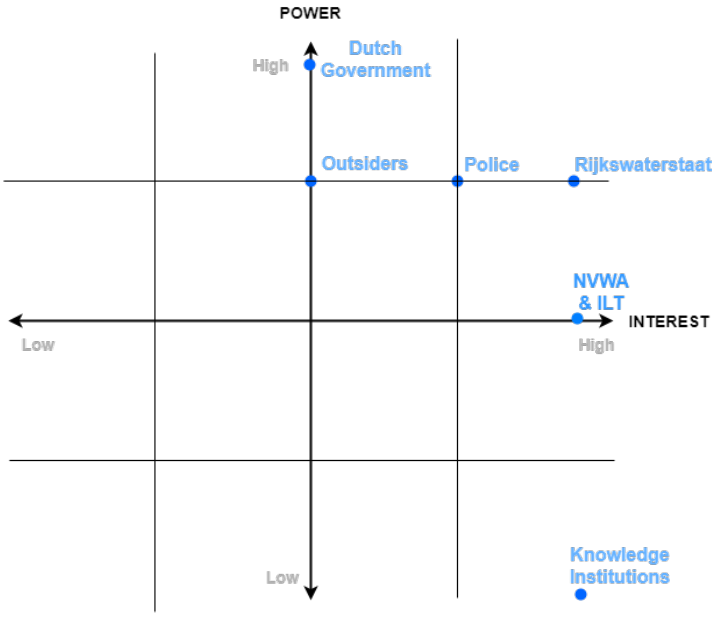


Figure 4.8: Power-Interest Matrix of involved stakeholders

4.2. Value Map

Stakeholders have different ideas about what is seen as ’the real problem’ which implies that the solution they provide is based on their shared value (Kreuter, De Rosa, Howze, & Baldwin, 2004). Responsible innovation hence requires the identification of the relevant public values, which is the final part of the Socio Technical Value Map. By doing this, potential value conflicts are analysed, and the working and acceptability of the technology can be improved (Von Schomberg et al., 2013). The values can be identified and worked out based on the findings of the main parties, discussed in the social map.

4.2.1. Efficiency

The most important motive or value of the parties using the technology, e.g. NVWA, ILT, Rijkswaterstaat and Dutch Police Department, lays with the agile, efficient and accurate drone characteristics. Values such as ”Lower Level of Human Interaction”, ”Faster Parcel-scanning/Detection Rate” and ”Fast Incident Control/Prevention” have been mentioned by multiple interviewees, indicating the various opportunities the technology offers. This has also been indicated in Chapter 3. Most of these values have the same underlying value; higher efficiency.

4.2.2. Safety

Drones are physical and flying objects which could form a risk to pose harm to the environment or individuals nearby. Technology developers in combination with the knowledge institutions (Saxion & WUR) and legislators (Dutch Government) value drone safety in terms of preventing incidents as a top priority. Safety guidelines and regulations stated by the European Union Aviation Safety Agency (EASA) and the Dutch regulatory framework should be used as a bench mark for ensuring one’s safety. Now in this context, individuals cannot simply accept the risk by making use of the service. When a drone harms one’s safety level, for example by crashing into someone or one’s property, there was usually no accepted risk of the drone operation by that individual. Cawthorne & Robbins-van Wynsberghe (2020) define this as a ”potential violation of the right to informed consent, which is grounded in the principle of autonomy” (p.9).

La Cour-Harbo (2019) quantifies the ground impact fatality rate of unmanned aircraft and judges the true reliability of drone detecting services yet to be ’undetermined’. Moreover, he mentions that fatality estimates require many assumptions and best is to mitigate this by flying in ’safety corridors’ to avoid populated areas hence reduce individuals’ exposure to safety risks (la Cour-Harbo, 2019). Please note however that the NVWA’s current operations are mainly performed on rural areas (e.g. farmlands); ergo, less populated areas. The risk of exposing people on the ground to such safety risks is therefore already low. Solely the individuals’ property, e.g. machinery, is exposed to this safety risks which arguably can be overseen.

4.2.3. Innovate

Another main value identified is the urge to innovate, i.e. introduce new methods, ideas or products. Stakeholders involved such as ILT and the Dutch Police Department clearly stated there exists an urge to find new and innovative solutions for their current activities. S2 in Appendix A.2 explicitly states: ”We look for innovating inspection methods which is why it is decided to spend 70% of the working time on innovating”. S3 mentions the desire for innovative investigating techniques and wants ”a more stable implementation of drones within the various instances of the Police Department. This clearly shows the relevance of the value ”innovate” and hence must be taken into account.

4.2.4. Security

Another value identified and to be considered is the security of the system. With this value, various codes were found such as ”lack of trust”, ”privacy sensitive data” and ”lack of protocol”. Now, security risks can range simply from an employee’s laziness to the lack of protocol in the work process, e.g. the disruptive threats identified in Chapter 3. The drones’ capacity to collect and share data in a fast way, remains to conflict with its trustworthiness. Simple said, the drone with its collected data can be hacked which leads to the exposure of potential personal information. As said before in Chapter 3, in 2016 a data leaking scandal was reported whereby the world’s largest drone manufacturer (DJI) shared data with the Chinese authorities (BBC, 2017). The Dutch Government must therefore be careful when using Chinese drones; the risk of data leakage remains to exist and can do great damage to the technology’s trustworthiness and public acceptance. The technology hence must be proven to be secure such that the trustworthiness and public acceptance is increased. These values are of great importance for further implementation, as mentioned by the Rijkswaterstaat (S3).

4.2.5. Privacy

Although this value hasn’t been explicitly stated by most stakeholders, privacy is one of the most important values to be taken into account of the use of drones. Codes such as ’privacy sensitive data’ and ’lack of protocol/transparency’ are closely related to the two values security and privacy. As mentioned in Section 3.2.1, the main issues of the digitisation era are associated with privacy, data protection and ethical issues. The device’s capabilities, i.e. payload options, to monitor and collect tons of imagery/video data can potentially harm an individuals privacy. For this reason, the privacy rights are enshrined in the Dutch Constitution and the EVRM (Custers et al., 2015). The Dutch legal framework offers various legal guarantees to enhance one’s privacy and safety level in this way. However the increase in popularity and lack of management makes enforcing difficult and leads to adjustments in the Dutch legislation. Especially for the stakeholders defined as outsiders, privacy is an important value which must be carefully embedded in the redesign. Privacy assessments and increased transparency in the operations might be a solution to control the increasing popularity of this technology hence increasing risk of privacy sensitive information exposure.

4.2.6. Reputation

Reputation is another main value, mentioned by multiple stakeholders during the interviews. Most of the stakeholders are governmental agencies which have great responsibility and a high level of expectations in the Netherlands. More specifically, they work on the basis of trust among the Dutch Government and the regular civilians. Quoting interviewee S4 from the Dutch Police Department in Appendix A.1; ”while innovating we must realize we play a big role in the Netherlands and hence have a great responsibility, and reputation”. S3 from the Rijkswaterstaat specifies this with giving an example of a potential incident with drones. ”If something goes wrong and the media takes notice of this, we will have to start all the way from the beginning again”, as stated by S3 in Appendix A.1. Trust will be lost and takes years to regain. This indicates the high dependency of public acceptance of the technology.

5 Responsible Redesign

As a recap, Chapter 3 concluded with the visualisation of the current work process and some vulnerabilities identified. The vulnerabilities were found in the last two stages; Operation and Processing. More specifically, bottlenecks were found in the current blurring techniques, data storage methods and its safety protocol. Furthermore, Chapter 4 concluded with a value map where the most relevant public values were analysed based on the findings of the main stakeholders involved. This led to a classification of six main values; Efficiency, Safety, Security, Privacy, Innovate and Reputation.

Now that the bottlenecks and critical values for the further implementation of drones are identified, the artifact must be redesigned. According to the DSRM by Peffers et al. (2007) the desired functionality, its architecture and the creation of the artifact, is key here. The artifact is in this case defined as the work process and must be redesigned in such a way that a research contribution is encapsulated in the design. The bottlenecks are connected to the most relevant values found and used as an input for the redesign. The proposed redesign will then mitigate the bottlenecks while simultaneously taking into account those values, hence be responsible.

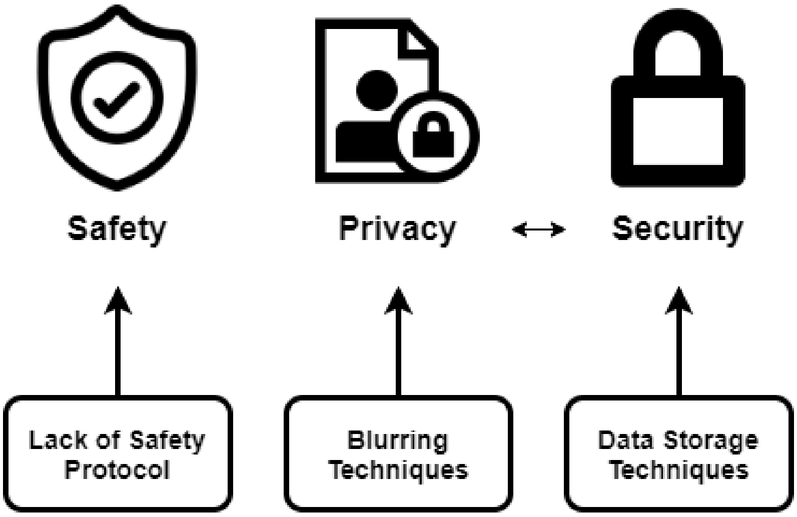


Figure 5.1: Linkage between bottlenecks identified and relevant values

5.1. Technology Trade Off

For the redesign, a trade off is performed on three different security techniques; Multi-Factor Authentication, Encryption and Blockchain Technology. In the following subsections, the security techniques are defined, described and assessed by means of a SWOT-analysis. SWOT stands for Strengths, Weaknesses, Opportunities and Threats, and is a strategic planning tool, companies can use for assessing a new business model or transformation within the organisation (Gurl, 2017). In this case, the new security technique capable of mitigating the bottlenecks found, is assessed. Strengths in the SWOT analysis are the positive factors of implementing the discussed technique, relevant for the organisation in the internal environment. Similarly, weaknesses are the negative factors that could hinder the organisation's performance in the internal environment. Opportunities are the factors that could benefit the organisation in the external environment. Think about advancements through which the organisation can exploit their advantages. Lastly, threats are the potential negative factors in the external environment that can hinder the goals on the long term. (Gurl, 2017) At last, a final choice is made based on the best performing security technique. Important factors such as reliability, usability and sustainability are covered and used as a measure for the final trade off.

.

5.1.1. Multi-Factor Authentication (MFA)

One technique to mitigate the bottlenecks found while taking into account the most relevant values is to use strong user authentication. According to (Cimpanu, 2019) almost 80% of data breaches are caused by compromised passwords, indicating that passwords alone are not sufficient. Users have too many accounts or a bad memory which often leads to the use of rather weak passwords. Especially when working with sensitive information this can cause huge organisational damage. Multi-factor authentication (MFA) however adds an additional layer of security and thereby reduces risk of data breaches. Moreover, it enhances the values security and privacy. The tool requires users to provide a secondary authentication such as a security token or biometric factor, in addition to a password. (Authy, n.d.) The secondary authentication is unique for each individual and therefore more difficult to 'crack'. Using this secondary authentication is rather easy since its simply a token, shared secret or biometric factor. Any time a user requests access to the database, the system will ask for the security token and grants access if filled in correctly. Before jumping into the SWOT-analysis of MFA, please note that the points listed are assumed to hold for every secondary authentication method, i.e. security tokens, biometrics et cetera. In reality, SWOT may differ per secondary authentication method.

Strengths

The strengths of MFA are of course related with the extra layer of security this technique provides. Users will have to identify themselves more than solely a username and password, enhancing the organisation's security. Companies such as Microsoft, Authy and Google offer different options of authentication which can simply be implemented in the organisation, e.g. security tokens or biometrics. It is widely available and is relatively easy to set up and use. Concerning the reliability, Microsoft mentions that users who enable multi-factor authentication for their accounts will block up to 99.9% of automated attacks (Cimpanu, 2019). The security technique is hence proven to be reliable and usable. Moreover, implementing MFA will meet regulatory compliance and assures a user identity due to the secondary authentication code. Moreover, using MFA indicates the organisation is aware of security concerns hence takes security seriously. This will help increase the trust in the organisation for outsiders. (Authy, n.d.)

Weaknesses

A known weakness of MFA is the regular maintenance required to keep the security on a high level. Especially in case security tokens or shared secrets are used, this is a must. Regarding maintenance, there are some recurring costs such as licensing, administration and support which should be taken into account. There exist high maintenance resources which include high costs of database management. Most can be outsourced but means there exist a dependence on third parties in case malfunctions occur. Especially when working with sensitive information, this is not favored. (Press Release, 2006)

Other weaknesses have to do with the increase in log in time and complex implementation respectively. Straightforwardly speaking, MFA requires the user to fulfil an additional authentication check hence increases log in time. The implementation of MFA requires setting up an architecture and integrating it in the current system of the organisation. The cost hence depends on the complexity of the network infrastructure, vendor support and additional software required. According to Press Release (2006), the total cost of ownership for implementing a software approach to 25,000 users is approximately 0.7 million $ each year (Press Release, 2006).

Opportunities

General opportunities lay with the fact that this technique is simple yet a lot more effective than solely a password. The increase in digitisation makes MFA a good first step towards full security of an organisation's database. According to Coco-Stotts (2020), MFA has a steady market growth while an increase in advancements in biometric technologies is experienced. Since this is unique and rather easy to use, there exist great opportunities in this method of MFA. Similarly, software tokens and cloud-based authentication services are in progress. Relating to the NVWA, adding factors such as biometrics or software tokens as a secondary authentication method will increase overall security and complies with the security standards set.

Threats

Finally, the threats of the security technique MFA are discussed. MFA is vulnerable for common practices such as phishing and social engineering. According to Coco-Stotts (2020), there exist tools that can take the login session when an user within the organisation clicks on a link in a phishing e-mail. In this way, the adversary can bypass the authentication and get to the data. Simple solutions like a session duration parameter can solve this, however might not be favored by the regular users of the organisation. This might hence be a threat for further implementation.

On the other hand, social engineering is a common practice by adversaries whereby users get manipulated in sharing their personal information such as secret tokens/passwords. Especially non-time sensitive codes can easily be shared and exploited by adversaries. Unfortunately, there is no technology yet that can tackle this issue. The only solution is to train the users of the organisation into recognising such cases and urge them to never share their credentials. (Coco-Stotts, 2020)

Lastly, as already mentioned in the weaknesses, MFA requires constant maintenance hence may experience design flaws. In case maintenance isn't done on a regular basis, adversaries could exploit a flaw in the system and do great damage. On the other hand, regular maintenance requires high cost and installation money for complex MAF models. This might be a barrier for implementation. (Coco-Stotts, 2020)

5.1.2. Encryption

Encryption, or cryptography, is another proven security technique that can greatly reduce the risk of unauthorised access. Encryption is a method that encodes data such that it can only be read by authorised parties. It uses algorithms to encrypt data and requires a key to decrypt and use the data. Similar as MFA, there are various forms of encryption. There exist different types of algorithms and methods of database encryption, such as Application Programming Interface (API), Plug-In and Transparent Data Encryption (TDE). Simple said, the difference between those has to do with the way it encrypts data. For instance, API encrypts in the application layer and uses API's to encrypt data before it is stored in the database. TDE is done on a database and Plug-In encrypts the database at a folder level. The latter is a common method of use due to its flexible usage in both commercial and open source databases. (OSS Encryption, 2016)

Strengths

The greatest strength of encryption is its adaptable nature. Encryption can be applied to almost all tech devices in use and ensures complete security, e.g. hard disk or file-based encryption. Moreover, it increases the overall security level since it is separated from the device security. This is because security is included within the encryption which permits administrators to store and transmit data via unsecured means. The data is encrypted on protected hard drives and together with the encryption keys in memory. (Matthews, 2020) Another strength is the increase in trust in the organisation by implementing encryption. Common encryption software providers such as IBM, McAfee and Vormetric start to grow and organisations worldwide are increasingly adopting encryption to protect their resources and improve its security level (Ashford, 2019). The main driver for using encryption is the need to protect data used and collected by innovations such as Internet-of-Things. However, another driver stated by Ashford (2019), has to do with the compliance of data protection laws, e.g. GDPR, and to increase trust and avoid reputational damage due to data breaches. Especially as a governmental agency, this is an important aspect. Lastly, encryption technology supports the integrity of the data by only letting authorised parties access the organisation's database and thereby decreasing the risk of an adversarial attack. Without the encryption key, there is no way to access the data. (Matthews, 2020)

Weaknesses

One of the main drawbacks of data encryption has to do with the maintenance and administration required. Simple said, the more users with encryption keys required, the more complex the administrative tasks of maintaining the keys. Users tend to forget their keys or experience bugs which could potentially lead to loss of data. Regular maintenance is therefore required and comes with recurring cost. In case of shared keys, loss of keys might not be an issue however the security of the encrypted data and its integrity might be questioned. (OSS Encryption, 2016)

Furthermore, like any other digital security, advances in computer technology and software, force the system to constantly update in order to remain 'unbreakable'. Bypassing techniques like brute-forcing and hashing for keys appear to work for weak encryption hence must be avoided. For this reason, a weakness is the false sense of security when using encryption. (Spamlaws, n.d.)

Lastly, encryption might be experienced tedious. Especially in cases whereby files need to be used and revisited often, encrypting and decrypting can be experienced tedious and could lead to users bungling the encryption protocol. (Spamlaws, n.d.)

Opportunities

Opportunities differ per type of encryption but can be generalised as promising. According to (MarketsandMarkets, 2020), the cloud encryption segment is the fastest growing in the market due to the increasing demand for securing sensitive information. Cloud, which is yet to be implemented by the NVWA, is increasing rapidly and therefore opportunities lay ahead for cloud encryption. Moreover, the global encryption software market size is estimated to grow from $ 9.8 billion in 2020 to $ 20.1 billion by 2025 (MarketsandMarkets, 2020). The growth can be linked to the growing awareness towards digital security threats among organisations worldwide.

Further, the importance of encryption is that in case an encrypted disk is lost or stolen, the encrypted data remains unchanged and only authorised users can decrypt it. Thus, even though an adversary gets its hands on the disk, the data cannot be read nor leaked.

Lastly, due to the increasing demand, an increase in encryption software providers is experienced and they start to compete with each other by offering more cost-effective solutions. This is of course a great opportunity for organisations to start adapting encryption in their practices. (MarketsandMarkets, 2020)

Threats

Like most security techniques, encrypting data does not ensure full security forever due to the constant evolving of technologies and bypassing techniques. As Spamlaws (n.d.) stated, database security managers are required to do regular maintenance and secure sensitive data within an organisation. Daily reviews of the database audit logs are necessary to make sure no data misuse has occurred. Besides, the manager provides access control for different users and assesses the programs that interact with the database. Only when these controls are performed regularly, the security of the database is enhanced and threats are avoided. This indicates that regular maintenance is key here. (Spamlaws, n.d.)

Logically, regular maintenance comes with recurring costs. Since there are many providers of encryption and the cost depends on the organisation's wishes, a concrete number cannot be given. According to Ashford (2019), full disk encryption can be around $ 230 per user, per year. Note that this however is not an accurate estimation since encryption can be made as complex as the organisation desires.

A concrete threat mentioned by Spamlaws (n.d.)is when a device/computer is set in sleep mode, often sessions are stored in the memory, making it easy for adversaries to retrieve data by scanning the memory for the encryption keys. This hashing process is done fast and easy depending on the complexity of the encryption. This again stresses that the implementation of encryption hence requires a protocol of action and degree of complexity, in order for the data to remain secure. The main threats are hence similar as MFA, related to the lack of maintenance and recurring costs.

5.1.3. Blockchain Technology

Blockchain is a technology and data managing method that allows users to validate, maintain and synchronize the content of a transaction ledger which is replicated across the other users (Tapscott & Tapscott, 2017). Moreover, it is a peer-to-peer enabled network where each participant can connect with another using secure cryptographic protocols, i.e. encryption. Just like encryption, there are multiple types of blockchain; public, private or consortium (Takyar, n.d.). In a public blockchain, anyone can join the network and gain access to the records in the blockchain. On the other hand, in a private or consortium blockchain there exist restrictions on who is allowed to participate in the network, i.e. gain access to the records. Private blockchains are often within one organisation while a consortium blockchain consists of multiple authorised parties. (Lastovetska, 2021)

Strengths

The strengths of a blockchain solution lay with its decentralised, distributed and immutable nature. Unlike conventional databases, blockchain is an open and distributed database (i.e. duplicated across many 'nodes' or computers), and is entirely decentralised. In other words, not one person or entity has control over the blockchain, making the database transparent. The data is maintained by all users in the blockchain ledger and has no single point of failure due to its distributed nature. All the nodes contain the same information allowing users to view the entire blockchain from his/her own device. Each block contains data with its own unique reference number (i.e. hash), time stamp and a hash of the previous block. In this way, each block has access and can communicate with its previous blocks down to the chain. (Tapscott & Tapscott, 2017) Moreover, a blockchain network promises 100% to all participants in the network. This means data cannot be tampered and a higher level of trust is obtained.

Weaknesses

Drawbacks or weaknesses of a blockchain network are mainly caused by its novelty. According to Higginson, Nadeau & Rajgopal (2019) blockchain is in its early growing stages of its life-cycle, meaning the technology is growing but not yet mature enough for standardisation. This also means that the implementation comes with greater cost. Logically, the operation system (OS) must be maintained/updated regularly in order for the system to run smooth without errors. According to (Takyar, n.d.), new OS updates are pushed every year, leading to a maintenance cost of approximately 15-25% of the overall project cost. No exact number can be given since it depends on the organisation's design requirements, i.e. the complexity of the system. Please note however that due to the system's distributed nature, a faster and more neat rate of maintenance of the system's records is obtained. More specifically, each block has its independent information which makes maintenance per block possible without data being corrupted or lost. Also, blockchain works with self-maintenance, meaning that users have to maintain their own wallets or else they lose access. However, in the case of a private network this would be different. (Gatteschi, Lamberti, Demartini, Pranteda, & Santamaría, 2018)

Another weakness is the relatively slow performance. In case a request is made to access the database, authorised users must validate the 'transaction' before access is granted. This is positively affecting the security however negatively affecting its performance.

Opportunities

According to Higginson, Nadeau & Rajgopal (2019), blockchain is in its early growing stages of its life-cycle. There is a growing market demand that leads to product standardisation and enhancements. In other words, the market size hence the availability of the technology is rapidly increasing, indicating widespread availability. Blockchain providers such as IBM and Oracle start to grow, while widespread application at scale has not yet been seen. This means there is room for a competitive advantage by adopting blockchain within the organisation.

Subsequently, blockchain allows the availability of heterogeneous data since many individuals can make use of it and share their data. This opportunity however depends on the type of blockchain network the organisation desires to use. Public means a lot of data and open access, while private means only the authorised parties may use access the database hence less heterogeneous data.

Threats

Potential threats have been implicitly stated in the weaknesses already and are related to its maturity and cost. The system could be perceived as unsecure or unreliable since wide-scale diffusion hasn't taken place yet. In other words, the technology is not seen as a standardised database security technique worldwide which could impose concerns. External actors such as governments can perceive blockchain as 'too risky' or 'dangerous' and therefore be seen as a threat for further adoption.

Subsequently, the cost of implementing a blockchain network is relatively high compared to a traditional database. The difference is simply because blockchain is a relatively new technology and still at its early stages in the life-cycle (Takyar, n.d.). For instance, additional costs of coding and testing the blockchain will be inevitable. Please note however that blockchain can arguably be more cost effective in the long term due to its decentralised structure.

5.1.4. Final Choice

After working out three common security techniques of this century, a final choice is made and justified. Based on the SWOT analyses performed before, the techniques are assessed on the following criteria; reliability, availability, ease of use, maintainability, sustainability, relative cost and novelty. Note that the latter is added as an extra criterion for the purpose of this report. A score is given per criterion, where a '+' indicates the technique performs good on that criterion and is favourable, '+/-' indicates average and '-' indicates the technique has a poor performance on that criterion and is not favoured. For example, a '+' for relative cost indicates the security technique has a relatively low cost which is favourable for the organisation.

In the case of the NVWA, multi-factor authentication is an interesting technique which has partly been implemented within the organisation already. However, after analysing this technique using SWOT, it is found that the technique might not be sustainable in the long term. According to Authy (n.d.), MFA is not 100% secure hence not risk-free. Especially with the NVWA's future plans and current experiments in EU projects as mentioned in the interviews, failure of MFA might be catastrophic. Another negative as seen in Table 5.1 is the fact that multi-factor authentication requires constant maintenance and can be experienced time-consuming by the users. In order for this technique to work, each user must be willing to verify his/her identity each time when logging in. If not, the reliability and the organisation's integrity might be questioned. Also, novelty has been given a low score since this technique is known and used by many organisations already.

Then, encryption would be a good start for the NVWA towards full security. Especially Transparent Data Encryption (TDE) which solves the problem of data at rest and encrypts data on the hard drive. Since the NVWA's current operations make use of hard drives and SD cards, this would be a fitting solution. Note however that on the long term, this wouldn't be sustainable in case NVWA decides to make more use of cloud and/or other data storage techniques. TDE doesn't encrypt data in transit hence might be an issue for future (autonomous) operations. Fortunately, cloud encryption methods exist which must be analysed in case cloud will be standardised within the organisation. In terms of usability, encryption requires a key, i.e. a password, to encrypt and decrypt data. The use is rather simple, however losing the key could potentially lead to catastrophic outcomes, e.g. losing the data associated with it. Also, bugs can emerge in databases and/or advancements in technology may obsolete old algorithms, making encryption a weak security technique. Encryption's reliability and sustainability may hence be questioned on the long term.

Lastly, blockchain was assessed. As seen in the SWOT analysis and Table 5.1, this technique scores positive on almost every aspect. Blockchain is a radical yet useful data managing method that is still in its early stages. This can be experienced both negative and positive; high cost but low amount of competitors. Although the NVWA doesn't work in a highly competitive environment, it would be an interesting first step if they start the adoption of blockchain within an governmental agency. Furthermore, blockchain has proven to be reliable in digital transactions and allows 100% transparency. The growing market size implies a growing availability and probable long term sustainability. Moreover, the technology is very novel hence will be better understood and adapted over time. For this reason, blockchain technology is chosen for the final redesign. Although this technology might not be mature yet, its properties in terms of security and transparency are highly favored and believed to be the most suitable for mitigating the open issues found in this research.

Table 5.1: Three discussed security techniques assessed based on set criteria

	Multi-Factor Authentication (MFA)	**Encryption**	**Blockchain**
Reliability	+/-	+	+
Availability	+	+	+/-
Ease of Use	+	+	+
Maintainability	-	+/-	+
Sustainability	-	+/-	+
Relative Cost	+	+	-
Novelty*	-	+/-	+

5.2. Blockchain Technology

Now after the technology trade off, it is time to get into detail of blockchain technology and propose a redesign of the current process.

The first implementation of blockchain technology was performed by Satoshi Nakamato in 2008 (Popovski et al., 2014). Nakamato used this technology for his latest peer electronic cash system also known as Bitcoin. His motive was to find cryptographic proof on the concept of 'double spending'. More specifically, Nakamato linked transactions in a tamperresistant manner, such that the formed network allows the examination of the transaction history and thereby preventing a (Bit)coin has already been spend, i.e. preventing the double spending problem. Nowadays, this method is known as blockchain.

Table 5.2: Characteristics Traditional Database versus Blockchain Network

	Traditional Database	**Blockchain Network**
Authority	Centralised; one single administrator	Decentralised; all participants in the network have to validate action
Transparency	Centralised nature implies low transparency	100% transparency by all participants in network
Performance	Fast and good scalability	Relatively slow due to verification/consensus method
Architecture	Client-server	Distributed ledger network
Integrity	Data can be altered or removed	Immutable nature
Cost	Low due to its common nature	High due to its novel nature

As noticeable in Table 5.2 and the trade off conducted before, the cost of implementing a blockchain network is relatively high compared to a traditional database. A traditional database is mainly for organisations who want a fast and cost-effective database system. However, a traditional database doesn't offer the desired transparency and integrity features. The difference in cost is simply because

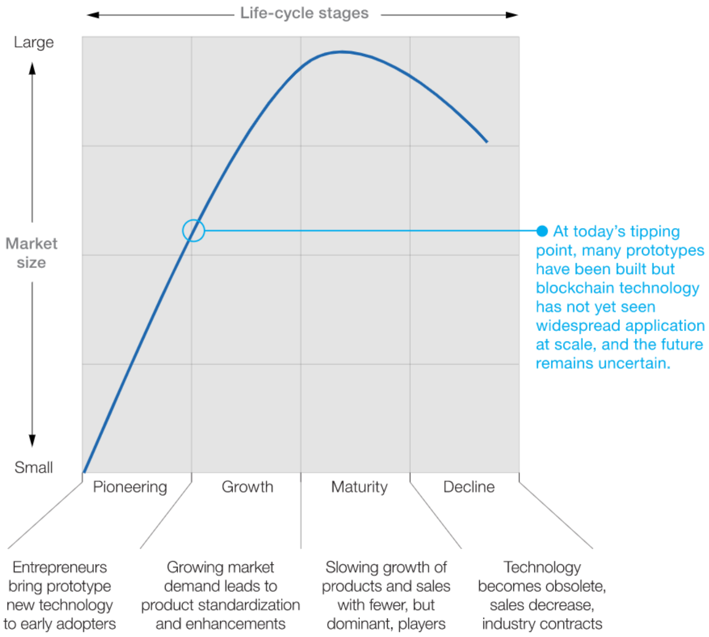

Life-cycle stages
Large
Market size
Small
Pioneering
Growth
Maturity
Decline
At today's tipping point, many prototypes have been built but blockchain technology has not yet seen widespread application at scale, and the future remains uncertain.
Entrepreneurs bring prototype new technology to early adopters
Growing market demand leads to product standardization and enhancements
Slowing growth of products and sales with fewer, but dominant, players
Technology becomes obsolete, sales decrease, industry contracts

Figure 5.2: Schematic view of life-cycle stages versus market size of blockchain technology (Higginson, Nadeau & Rajgopal, 2019)

blockchain is a relatively new technology which is still at its early stages in the life-cycle, as seen in Figure 5.2. In other words, a small amount of entrepreneurs bring prototype new technology to early adopters, however the market size remains small (Higginson, Nadeau, & Rajgopal, 2019). This also means that this group of entrepreneurs has a competitive advantage and can therefore set the price for implementation. Their knowledge of blockchain can be seen as rare and valuable for nowadays public. However, the growing demand for blockchain can arguably lead to more cost effective solutions in the long term. (Iredale, 2020)
Now connecting blockchain to the research problem; the goal is to improve the work process of drone detecting services such that a more responsible adoption rate is achieved. To do this, bottlenecks and open issues were found and must be mitigated. As indicated earlier, bottlenecks are found in the operation and processing phase of the work process. Important values such as safety, security, privacy and reputation are related to these issues must be included in the solution. There are three key characteristics of blockchain technology that show why blockchain can mitigate the bottlenecks; distributed, decentralised and immutable. These are highlighted and will be discussed in the next subsections.

5.2.1. Distributed Ledger

As mentioned before, the ledger (or book of records) is shared across all instances in the blockchain network. Meaning, every stakeholder or participant in the network has full access to the ledger on an independent base. (Tapscott & Tapscott, 2017)

For drone operators to perform their flights in a safe and efficient way, a brief preparation phase is performed including safety checks and area mapping. In an oversimplified form, this is done by area mapping, getting permits required and making the flight plan accordingly, days before the actual operation. Simultaneously, safety checks are performed by checking weather conditions, checking for NOTAMs and other external risks in the air or nearby environment. The drone operators are required to share their intended flight maps and any route changes with the airspace authorities. These flights maps or plans must be accurate and up to date in order to prevent conflicts or incidents with other aircraft. In other words, real-time awareness is critical to ensure the safety.

This is where blockchain comes into play. When using blockchain, the process of sharing accurate flight data is simplified due to its distributed nature. The drones and operators can be equipped with each a unique ID (similar to the Remote ID discussed in Chapter 3) and can share real-time information throughout the participants in the network. For instance sharing its status, flight details, the operator and of course its flight and maintenance history. Since the system is distributed, there is a built-in redundancy and it updates data real-time, making the system more secure. Both flight and situational awareness is provided such that the individuals' safety is enhanced and risks are mitigated.

5.2.2. Decentralised Structure

By using blockchain technology, there is not one single individual responsible over the network. All participants are present in a network with similar responsibilities and authorisations. In other words, a decentralised structure is obtained as illustrated in Fig 5.3B. This also means there not one single point of entry for adversaries, making the database more secure. The records are not processed by one central administrator, but by a network of users who are expected to verify the data and together come to a consensus. In other words, a peer-to-peer (P2P) network. In this way a history of activity is obtained rather than a snapshot in time. The distributed essence and independent information of each block allows a fast maintenance of the system's records without data being corrupted or lost. This means higher transparency in the process, allowing tracing back for the users in the network. Tampering or altering data is hence noticeable by all users in the system. (Lastovetska, 2021) Also, the increase in transparency in the network and database allows authorised parties such as the governmental agencies to access and check if operators are enforcing the regulations set. Please note that solely authorised parties will have access to this data by means of a private key, i.e. decryption key. (Lastovetska, 2021)

Also, a decentralised structure means no resources have to be spent on a central administrator or intermediaries. This might not be the most interesting benefit in this context, however must be mentioned. Subsequently, so-called smart contracts can automatically trigger actions on the blockchain which automates the administrative work, hence reduces time and cost. This will be further explained later on.

5.2.3. Immutable Ledger

Another key aspect of blockchain is its immutability. Blockchain allows records (i.e. data) to be logged in a ledger which is verified by the participants in the blockchain network, timestamped and embedded into a “block” of information. This is then cryptographically secured by a hashing process that links to and incorporates the hash of the previous block, and joins the chain in a chronological order. Now the link in the hashing process, between the two blocks, makes it impossible to alter or remove data after validation by the network. An attempt of alteration or removal would immediately be noticeable by the other blocks hence the users in the network. In other words, the chain would be broken and the root cause can be easily identified. Conventional databases, data can be easily altered or removed, making the system less secure. (Doubleday, 2018) In this way, higher security and potentially a higher trustworthiness in the organisation is obtained. As indicated in Chapter 4, this is highly favored by the governmental agencies. Besides, in case of an accident they need assurance that the flight log-

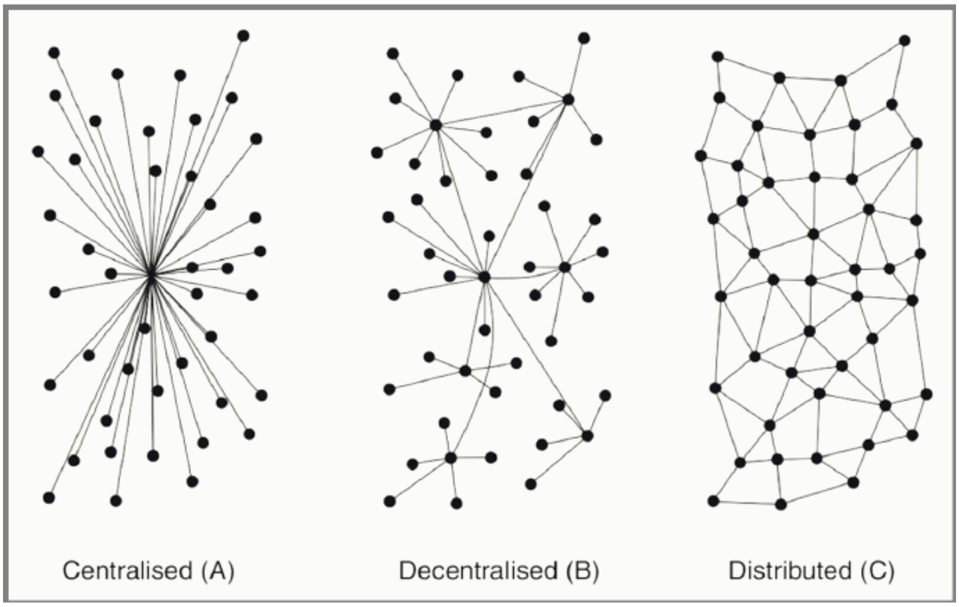


Figure 5.3: Centralised, decentralised and distributed network models by Hoelscher (2014)

book/data has not been altered or tampered with by the operator. Blockchain's immutable nature hence ensures the security and integrity of the data exchanged between the participants in the network, e.g. drone operators and the governmental agencies.

5.2.4. Automated Compliance and Protection Mechanism

Besides the three key characteristics, it is important to highlight its automated compliance and protection mechanisms against adversarial attacks. This is where smart contracts come in play. Smart contracts are defined by (Tapscott & Tapscott, 2017) as ”software that mimics the logic of contract with guaranteed execution, enforcement and payments”. The implementation of blockchain with its smart contracts will ensure that all drones and its operators follow the (national) regulations. The regulations or rules can be encoded into the drone's system such that it can plan and execute its operations based on the standards set, e.g. no flight zones and altitude limits. The use of smart contracts will ensure safety standards are met on an automatic base. A safety protocol will hence not be needed once the safety standards are embedded in the contract. This mitigates one of the obstructions found in Chapter 3; lack of safety protocol. Furthermore, its decentralised nature allows regulators or operators to add regulations per operation. For instance an operation in a rural area often requires different safety standards than in an urban area. Blockchain allows the flexibility of complying with these set rules before and during a flight operation with a changing environment.

Also, the smart contracts imposed by blockchain technology ensure the device and equipment (payload) is solely used when it is safe. More specifically, if maintenance is required, the smart contract makes sure this request is visible by the participants in the network and can only be resolved by an expert. In other words, operators cannot make use of the drone or equipment before the expert approves its safety and security. This can of course also be used to schedule and ensure monthly maintenance to reduce risks of system failure.

Furthermore, blockchain has a built-in protection mechanism due to its decentralised structure. Unlike a centralised system, there is not one single point of entry for adversaries, making it harder for them to attack. More specifically, assets are distributed across a global ledger using a high level of cryptography (i.e. encryption). When an action is conducted, it is posted globally across millions of computers hence noticeable by all users. If an adversary, e.g. a hacker, wants to perform an attack on one block, it must attack all the preceding blocks across millions of computers simultaneously. This is almost impossible and can therefore be seen as a built-in protection mechanism. (Higginson et al., 2019)

5.3. Preliminary Design

Since the motive of usage is clear, it is time to construct a preliminary redesign for a use-case by the NVWA. Before doing this a common blockchain architecture diagram is given in the form of a digital transaction. Any new transaction or record implies the building of a new block. In Figure 5.4 this is referred to as a transaction block. The record is proven and digitally signed such that its genuineness is ensured. After the creation, the block is send to all nodes in the network must be verified. When the nodes validate the transaction, a reward is given to them and the validated block is added to the existing blockchain. The record or transaction is then saved and completed. Please note that the example given is in the form of a digital wallet where actual transactions take place and nodes receive financial rewards. For the case of the NVWA, the nodes in the network mainly consist of stakeholders whereby transactions are not needed. This is merely done in a public blockchain, while the NVWA will mostlikely make use of a private or consortium blockchain. Straightforwardly, in a private or consortium blockchain only a selected amount of nodes can request records and gain access to the blockchain. (Lastovetska, 2021)

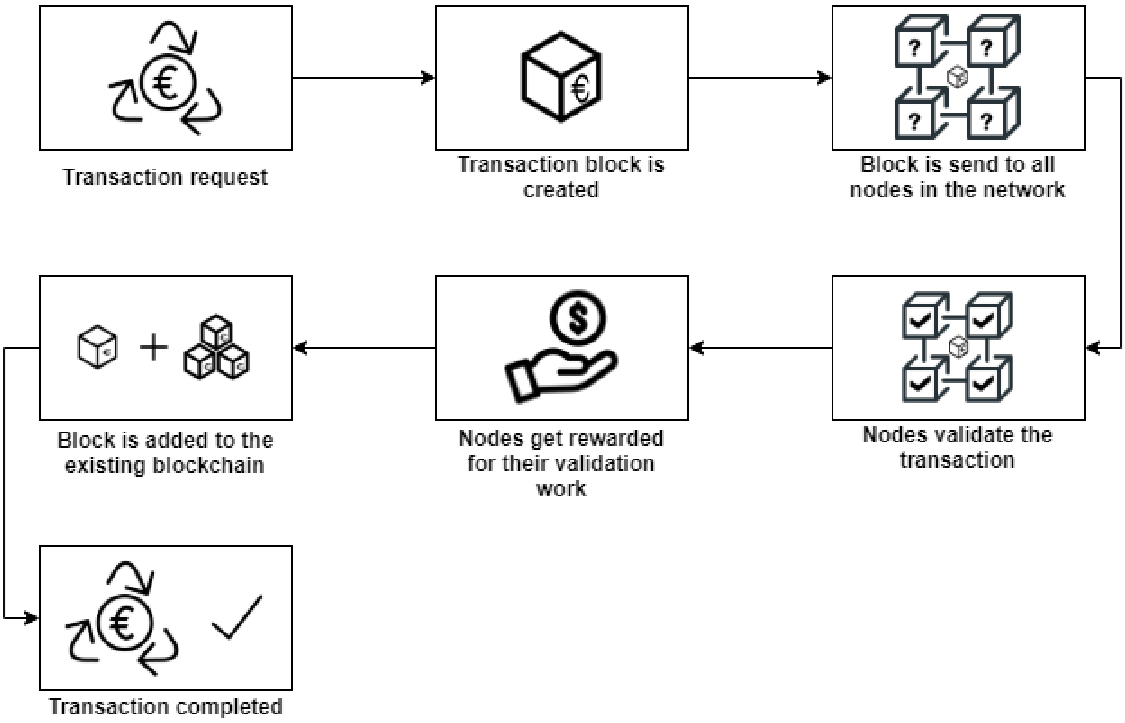

Transaction request
Transaction block is created
Block is send to all nodes in the network
Nodes validate the transaction
Nodes get rewarded for their validation work
Block is added to the existing blockchain
Transaction completed

Figure 5.4: Schematic view of a basic blockchain architecture for a digital transaction adapted from Lastovetska (2021)

An use-case architecture including a step-wise description will be given for two scenarios. The first one consists of a farmer wanting access to the collected data of his parcel. The second one consists of an authorised party, e.g. Dutch Government, who wants to gain access for incident inspection and prosecution purposes. Most likely, a private or consortium blockchain will be best for the case of the NVWA.

In a public blockchain, anyone can join the network and gain access to the records in the blockchain. On the other hand, in a private or consortium blockchain there exist restrictions on who is allowed to participate in the network, i.e. gain access to the records. Private blockchains are often within one organisation while a consortium blockchain consists of multiple authorised parties. (Lastovetska, 2021) Since the NVWA works with personal information, open access is not desired. For this reason, a consortium blockchain is proposed.

5.3.1. Use-case 1: Farmer

The first scenario contains two participants; the NVWA and a farmer/outsider. For the sake of clarity, first the components are described in short. Moving from left to right, the drone system (NVWA) is straightforwardly the operating drone(s) including its determined payload by the NVWA. The control system is the responsible component which receives data from the drone system, hashes (i.e. a form of encrypting) to preserve its integrity, and sends the hashed data record to the blockchain network. Moreover, it monitors, controls and sends out commands to the drone system. The blockchain network is where all the hashed data records are stored and can be accessed by means of smart contracts. The smart contracts are part of the blockchain and can perform actions when certain conditions are met. In the next figure, a simplified process of blockchain included is shown in a parcel-scanning drone operation. In this operation, a farmer wants to get access to the collected data for other purposes. A step-wise plan of action is written down below. Please note that this an oversimplified projection.

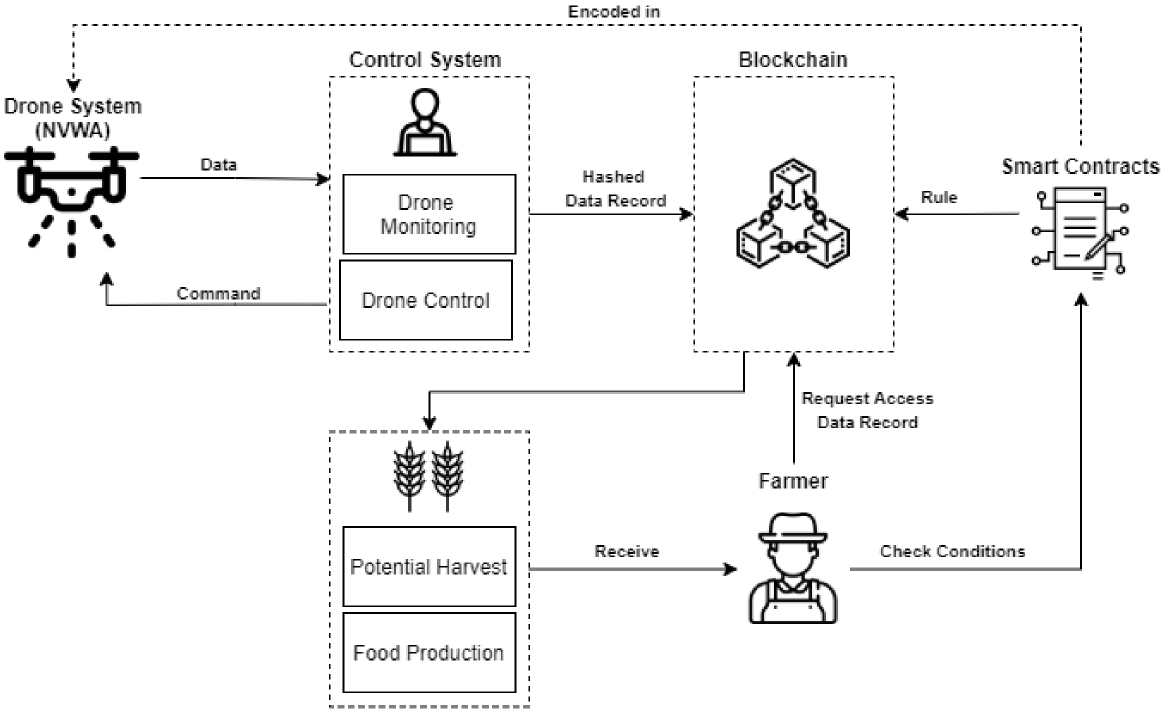


Figure 5.5: Use-case 1: Simplified process of how blockchain can benefit farmers in a parcel-scanning drone operation

1. Drone system performs parcel-scanning operation to determine the amount of cattle present. Imagery data is collected and received by the control system.
2. The control system controls and monitors the drone, makes minor adjustments if needed and receives the collected data by the drone system.

3. Subsequently, the control system hashes (i.e. a form of encrypting) the collected and command data, and sends this to the blockchain network.
4. The data consists of the commands, collected data and the device used (device ID) during the operation. This is then uploaded to the blockchain network and stored in a distributed (block-based) manner.
5. The landowner or farmer wishes to access the data record of his/her land, collected by the drone system. Allowance of access is checked in the conditions of smart contracts.
6. Green light is given in case private key is present and all users validate. The data record can be accessed and a (possible) transaction is made. Depending on the user agreement, a transaction is made to the other party in the network.
7. The farmer benefits from the data recorded by the drone system in a safe and transparent manner.

Now one may wonder if this won't affect one's competitive advantage against the other farmers. Since the database is transparent in other words visible for all participants, farmers could hypothetically exploit the service and use it as a 'spying' tool. Farmers could therefore be hesitant in taking part of the network because they will lose their competitive advantage. In case of an open blockchain network, this might be an issue. Please note however that every participant must verify the request before access is granted. This built-in protection mechanism makes accessing other farmers' data hard. However another solution could be to solely grant access to authorised organisations/parties which can communicate the data directly to a farmer when requested. In this way, a semi-centralised structure is set up while the other farmer's data integrity is enhanced. The RVO could be a good option since all farmers are registered in their database already. The RVO is a regulatory body of the Dutch government and provides information about financial and tax arrangements (RVO, n.d.). Farmers will need to request access to the database via the RVO. Potentially, a revenue model could be set up whereby farmers will need to pay for the data available.

5.3.2. Use-case 2: Authorities

Another use-case is shown below where blockchain allows authorised parties to access the (private) data records to ensure regulatory compliance of the drone operators. Apart from the different requesting party, the components are similar as in use-case 1.

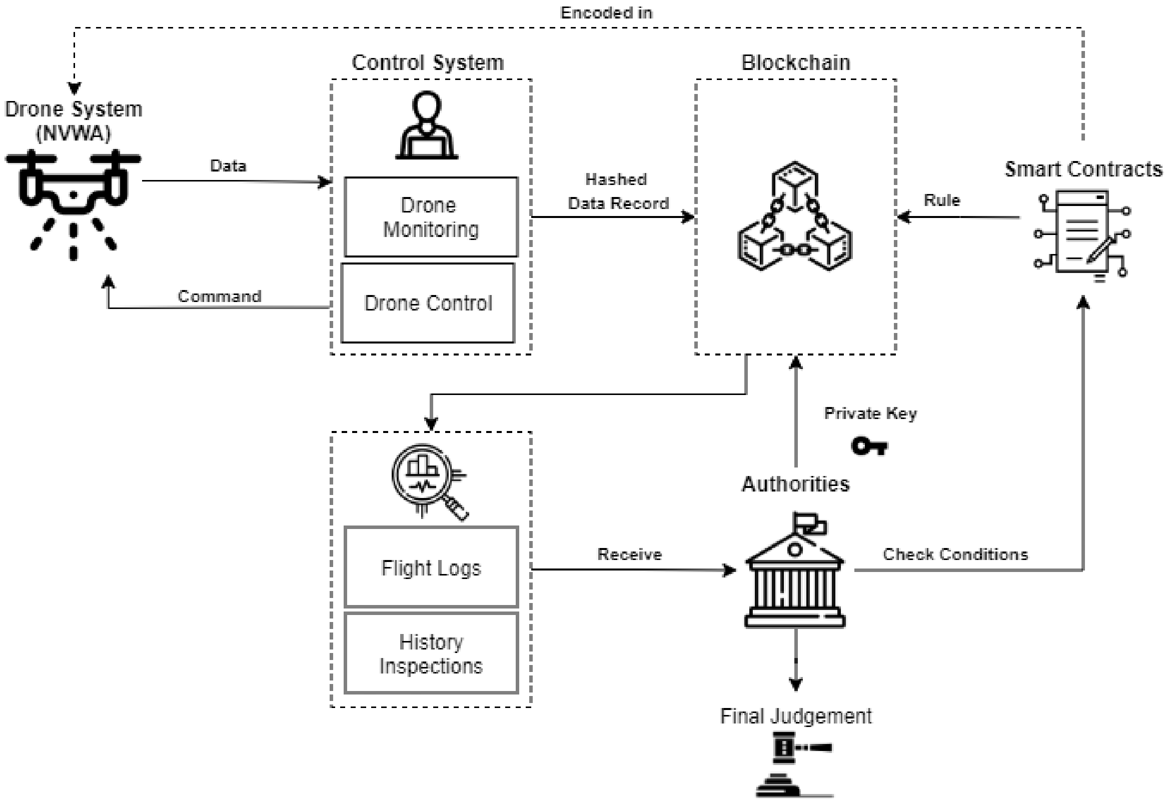


Figure 5.6: Use-case 2: Simplified process of how blockchain can benefit authorities

In this case, the private keys and authorised role ensures only authorised parties have access to the confidential data records such as flight logs and operator details. This can be used to give a final judgement for an occurred incident. Please note again that blockchain's immutable nature ensures the data is not tampered with hence is 100% reliable for the authorised parties.

An oversimplified view of the process is shown in Figure 5.6. A step-wise plan of action is written down below.

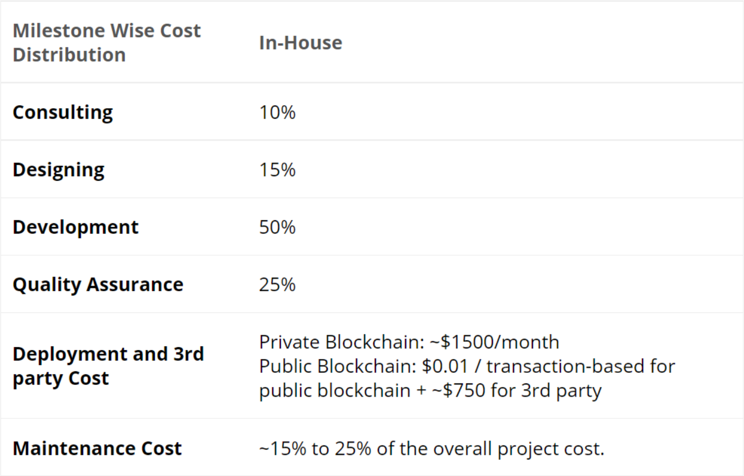
1. Drone system performs parcel-scanning operation to determine the amount of cattle present. Imagery data is collected and received by the control system.
2. The control system controls and monitors the drone, makes minor adjustments if needed and receives the collected data by the drone system.
3. Subsequently, the control system hashes (i.e. a form of encrypting) the collected and command data, and sends this to the blockchain network.
4. The data consists of the commands, collected data and the device used (device ID) during the operation. This is then uploaded to the blockchain network and stored in a distributed (block-based) manner.
5. An incident has occurred so an authorised party requests access to the data record of the drone system active in that area. Allowance of access is checked in the conditions of smart contracts.

6. Green light is given in case private key is present. The data record can be accessed and a (possible) transaction is made. Depending on the user agreement, a transaction is made to the other party in the network.
7. The authorised parties determine when the incident took place, what equipment was used, who was in charge and make a final judgement based on the non-tampered data.

5.3.3. Development Resources and Final Remarks

To complete this analysis, a rough estimation for the required development resources of implementing a blockchain network is made. Please note that this includes assumptions which in reality might differ depending on the choices made of the organisation.

For this analysis, it is assumed the NVWA will make use of a consortium or private blockchain network. Subsequently, since the NVWA is a governmental agency, it is assumed a blockchain development team is hired. It is crucial to find professional programmers who will create and implement blockchain in the existing practices of the organisation. According to Davies (n.d), the following elements must be addressed; an infrastructure, storage space, network speed, P2P network, encryption, smart contracts and a front-end. Moreover, the cost of building a blockchain network depends on factors such as the type of blockchain, app features, complexity and platform of use.



Milestone Wise Cost Distribution	In-House
Consulting	10%
Designing	15%
Development	50%
Quality Assurance	25%
Deployment and 3rd party Cost	Private Blockchain: ~$1500/month Public Blockchain: $0.01 / transaction-based for public blockchain + ~$750 for 3rd party
Maintenance Cost	~15% to 25% of the overall project cost.

Figure 5.7: The cost percentage with respect to a specific development phase (Takyar, n.d.)

As seen in Figure 5.7, the main costs are formed in the development stage. According to Takyar (n.d.) a private blockchain is the most expensive type due to its complexity and customisation, and can cost around USD 1500 per month. Of course this depends on developing decisions such as outsourcing and platform of use. Moreover, the development phase consist of setting up the above mentioned elements such as the infrastructure, interface and smart contracts. According to Tarasenko (2019), an average project requires three to ten programmers who will create the blockchain network and perform the developing tasks. Their average cost of payment in Western Europe is around $ 70 - 100 per hour. Concerning smart contracts, the prices can differ depending on the complexity. Developing a simple smart contract, capable of serving simple operations of transferring values from one side to the other, will cost around $ 200 - 1,000. Advanced smart contracts that can additionally provide access to information and enter data into databases can cost up to $ 50,000 (Tarasenko, 2019). However, as Tarasenko (2019) mentions, each project for the implementation of the blockchain is unique and it is therefore impossible to indicate an exact cost value of the costs included.

5.3.4. Final Remarks

Concluding, as illustrated in the use-cases, blockchain technology is an innovative way of storing and sharing data and leads to a higher security level and more transparency in the process. The NVWA has a more secure database and can control who has access to it (in case of a consortium or private blockchain network). Moreover, it can get real-time information of its devices, the surroundings and other environmental factors due to its distributed ledger. Hashed data is stored in blocks, authorities can access the data records to ensure regulatory compliance and lastly, the farmers/outsiders part of the network can request access to the collected data for personal purposes, e.g. specific parcel information. The data is stored in a blockchain based database which is immutable hence reliable for all parties. Moreover, blockchain can be used to mitigate the current bottlenecks for further implementation of drones by the NVWA and could even lead to collaboration possibilities and revenue models in the future. Think about consortium formations, digitised inspections and other revenue models. More details about this can be found in the discussion chapter of this research. In Figure 5.8, blockchain's contributions to the open issues found in Chapter 3 are included. Note that the preparation phase won't be affected and is not included in this figure.

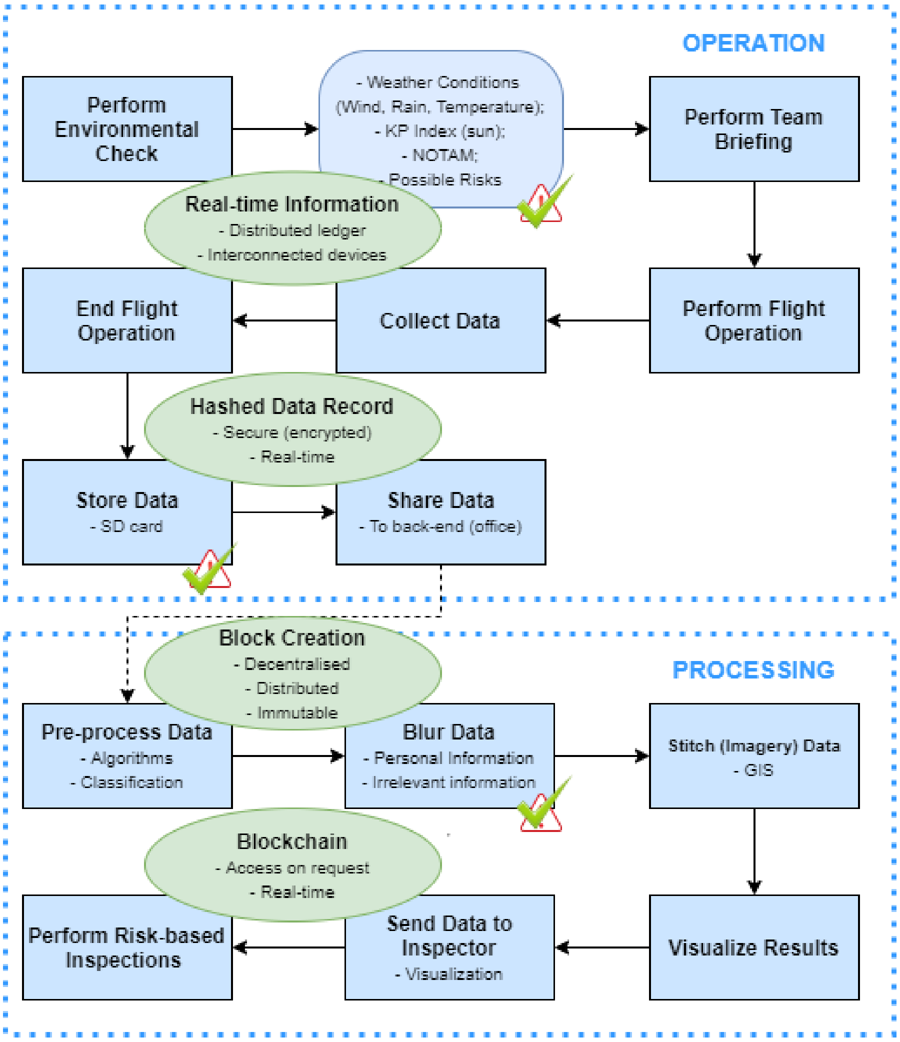


Figure 5.8: Schematic view of improved work process including contributions of a Blockchain solution.

6 Evaluation

Following the DSRM by Peffers et al. (2007), after the construction of a qualitative research and redesign proposal, an evaluation must be performed. The usefulness of the solution must be demonstrated and validated. Given the diverse genera and form of qualitative research, there is not one best-practice method for assessing a qualitative research work. Leung (2015) distinguishes between three different criteria; validity, reliability and generalisability. Validity is defined as the appropriateness of the tool. In other words, whether the design is a valid tool for answering the main research question and solving the knowledge gap. In qualitative research, reliability refers to the consistency of the research and generalisability refers to the degree to which the design can be applied in different contexts. (Leung, 2015)

Now since the redesign cannot simply be implemented and tested in practice, its validity and generalisability are tested by means of evaluative interviews. More specifically, two evaluative interviews of experts in the field of research are conducted. Reliability is assumed to be negligible for this evaluation.

6.1. Approach

Now as said, in order to test the design its validity, usefulness and generalisability, two evaluative interviews were performed. To do this, first a list of relevant questions was constructed. The questions were constructed in such a way that the interviewee could clearly give feedback on the design and indicate its validity and generalisability. The following list of questions was asked;

1. *Is it clear how blockchain improves the work process such that a more responsible adoption rate is achieved?*
2. *Is the proposed blockchain method useful to the organisation?*
3. *Is the method generalisable, i.e. applicable in other contexts?*
4. *What are the strengths, weaknesses and potential improvements of the design?*

After the construction of the questions, the participants for the interviews were chosen. This was done based on profession, experience and on previously conducted interviews. Moreover, only participants within the organisation of the NVWA were chosen such that a reliable evaluation was obtained.

The first participant chosen, had already been interviewed for the explorative mapping in Appendix A.1. This person is entitled as a Specialist Remote Sensing & Data Acquisition / Senior Inspector and is

part of the department Trade & Digital Surveillance. The individual's experience as senior inspector and specialist in remote sensing shows a high level of knowledge in the field of research. Besides, during the explorative mapping, input in terms of current obstacles were mentioned and used for the redesign, making evaluation a logical next step.
Subsequently, the Head of Department Trade & Digital Surveillance was chosen as the second participant. This person straightforwardly has a high level of responsibility and power as head of the department hence can give reliable feedback of the usefulness and generalisability of the design. For the sake of time and quality of the report, only two participants were chosen for the evaluation.

The interview went as follows; first background information was given in the form of a presentation about the performed research and issues found. When the knowledge gap was clear, the design concept was described in detail with two use-cases. The presentation ended with summarizing the benefits and the linkage between the main research question.

6.2. Findings

Now in this subsection, the findings of the two interviews performed, based on the four questions listed above, will be described in detail. The fully transcribed interviews can be found in Appendix A.3 Evaluative Interviews.

6.2.1. Clarity and Usefulness

The first questions were asked to test the clarity of the design and if it fulfills the desired purpose. Both interviewees were familiar with blockchain and found the design clearly described. They agreed that by means of a consortium blockchain, the system can be well secured for certain parties. Also, the use of a private key is a 'good' step towards automatising the database. The use-cases were very clear however it was suggested by one interviewee to provide access to the Netherlands Enterprise Agency (RVO) in stead of an individual farmer. They can be seen as the responsible/authorised party of the farmers such that not all individual farmers need to request access to the blockchain. This is an interesting point however makes the system again slightly centralised. Furthermore, the interviewees noted that the implementation of the system will be a challenge due to its complexity. Small steps towards the final blockchain design will be needed, was said. Nevertheless, the design was highly appreciated and a copy was requested for further purposes of the organisation.

Concerning the usefulness, it was agreed that the method will increase security and transparency in the process. Besides, the collaboration possibilities and future revenue models were highly appreciated for on-going projects. They referred to the subsidy projects of farmers whereby blockchain could allow a trustworthy transaction based on 100% reliable data.
Subsequently, the use-case with an authorised party was stated to be very useful for current obstacles regarding security and access management. Uncertainties were however found in the network validation check. The validation of all nodes in the network might lead to delays. The organisation must hence decide on which level, i.e. with which nodes, this validation will take place. This will also depend on the type of blockchain is used; private or consortium.

6.2.2. Generalisability

Additionally, the generalisability of the design was tested. Both interviewees confirmed its generalisable nature and favored a consortium blockchain such that multiple organisations could benefit. According to the participants, Blockchain's transparent and responsible method of data sharing can be used as a building block for the newly digitised inspections. A data-driven way of working is emerging and blockchain could create great value here. It is noted that some generic is required in the smart contracts. In this way, accessing and sharing data could be made more easy. The interviewees also referred to the existing projects, e.g. Drone2Go, where they desire to form a consortium of various parties using drones in the Netherlands. The interviewees agreed that blockchain could be the next step towards forming this consortium hence creates value for different parties in different contexts.

6.2.3. Strengths & Improvements

Straightforwardly, both interviewees listed improved transparency and security as the top strengths of the design. These remain the current main issues hence would be extremely helpful when improved. Besides, the interviewees liked how the use-cases showed the technology could actually work hence is applicable and logical in different contexts.

For the improvements, the technology's maturity was criticised, making it difficult to implement. Besides, the laborious validation check by all nodes might take too long for gaining access to a simple data block such as imagery of a forest. One interviewee mentioned that if you had to validate every picture on a data block, it will be extremely time-consuming. Hence clustering the data might fasten this process such that clusters of e.g. forests can be shared faster. An agreement was made that clustering and/or scaling the data in terms of sensitivity could potentially increase the validation process, leading to faster data sharing/access. Lastly, there were some concerns regarding the acceptance and dependency of the NVWA's supervisor referred to as ”The Hague” and ”Brussels”. The governmental bodies must be convinced before this technology can be implemented on a large scale.

6.3. Summary

To validate the design, an evaluation was performed based on the interviews of two experts. In this interview, aspects such as clarity of the design, usefulness, strengths and weaknesses, and the generalisability were tested. The interviewees responses were positive and coherent. The design was well-structured and the idea and usefulness were clear to both participants. Besides, both participants liked the use-cases and agreed the concept is generalisable. Revenue models and future collaborations were discussed on the side. In fact, a formal approval was given for the use of the use-cases, hence design, for future purposes of one of the participants. This clearly indicates the design is valid hence beneficial for the organisation. The strengths were clear although some weaknesses/improvements still exist in the implementation of the technology. This is mainly due to the technology's maturity and the required permission of the governmental bodies in the Netherlands.

7 Discussion

The research ended with the introduction of a responsible redesign by the use of blockchain technology. Blockchain technology is an innovative way of data management which is mainly characterised by its distributed, decentralised and immutable nature. These respectively induce a higher level of transparency and security in the process, which could make the implementation and use of drone detecting services more responsible. This answers the main research question and is recommended to be used by the NVWA such that a more responsible adoption rate is achieved. In this section further limitations and implications are addressed.

7.1. Limitations

While investigating the research questions, a number of limitations and other issues were encountered. This must be critically evaluated in order to conclude the research.

First of all, a major obstruction for the nationwide implementation of drones is indicated to be the Dutch legal framework. Multiple stakeholders and white papers have indicated the legal framework to be strict and conservative which obstructs the further roll out of the technology. Besides, governmental instances are responsible for financing the resources hence determine the budget available for the organisation. Subsequently, privacy and safety are important values of the Dutch government which is strictly taken into account in the Dutch legislation. Important to note is that the legal framework is constantly changing and tends to follow the EU guidelines also referred to as the EASA. This has been noticeable in January 2021, when the new EU guidelines for drones were adapted in the Netherlands. It is hence a challenge to increase the adoption rate while following the constantly changing guidelines and acting responsibly. Besides, different organisations have varying power in terms of implementing drones. The police for instance can implement drones faster than the NVWA due to the regulations set. This has to do with the criminal law which is an interesting future research. It is hence safe to say that the constantly changing Dutch regulations makes the future drone adoption hard to predict. Now as already stated by Custers et al. (2015), it is difficult to provide a detailed illustration of the future legislation due to the constant technical developments and the social and political desirability of making certain applications of drones both possible and impossible.

Now a more specific limitation regarding the redesign has to do with its maturity. As already said, blockchain technology is a relatively novel technology which is stuck at its pioneering stage. This means

that many prototypes have been built but blockchain technology has not yet seen a widespread application, making the future adoption uncertain. Simultaneously, the involved costs are hard to estimate which can be a limiting factor. Possible explanations have to do with the ignorance and unfamiliarity of the technology. Its disruptive characteristics in different contexts can lead to radical changes in an organisation which is often not favored. For this reason, many organisation are hesitant in implementing the technology. Besides, in the case of the NVWA, the technology is used for data management which means privacy sensitive data is used. As an governmental agency, this requires taking a big step and risk in using this novel and promising technology for solving the current open issues. This has also been indicated in the evaluation; the implementation is challenging and requires ’The Hague’ to be convinced.
However, taking small steps forward and keeping it as transparent as possible might solve this limitation. Perhaps first start constructing all smart contracts and deciding the consortium. That in combination with the Dutch legal framework will be yet another challenge to tackle.

Another limitation regarding the technology has to do with the potential delay experienced in the validation phase. When a consortium blockchain is chosen, multiple users or nodes will be present in the network, making the validation phase time-consuming. This could lead to delays and is inefficient for the process.

Regarding the research methods used, a limiting factor could be a potential bias in the interviews conducted. Most participants interviewed were chosen because of their familiarity with the concept and use of drone detecting services such that they could answer specific questions of the process. However the risk of using familiar participants has to do with potential biases in answers of the values and obstructions experienced. There might be a slight bias pro drone-use due to their experience and familiarity with the technology.
Also, the values and obstructions experienced by the responsible ministries were obtained via the governmental agencies and not directly via an interview due to its centralised structure and time constraints. Although it is believed to be correctly adapted from the interviewed stakeholders, for reliability a closely involved Dutch Minister should have been interviewed for the construction of the value map.
Subsequently in order to fix the bias, not only a bigger sample size (i.e. group of interviewees) but also a more diverse sample size should be taken. By also taking into account the less familiar stakeholders of the technology, a more reliable and realistic construction of potential obstructions and values could be obtained.

Lastly, another limiting factor for the implementation of the redesign has to do with the current COVID-19 pandemic. Straightforwardly, like any other activity, the operations by the NVWA have been on a hold due to the recent pandemic. This also means that the experiments for further application domains have experienced delays. Note that conducting experiments are of course crucial for the expansion of drone-use in the Netherlands.

7.2. Implications

A next discussion point has to do with the design’s future implications. In other words, how can this design be helpful and generalised in different contexts. A distinction was already made between revenue models and collaboration possibilities in the redesign and evaluation.

Now as seen in the definition of blockchain, the technology can be used to form a consortium between multiple stakeholders involved. By forming a consortium blockchain, and setting up the ’rules’ in the smart contracts, all stakeholders in the network can access and use the blockchain system for their own purposes. A long as all nodes or participants validate the transaction, a stakeholder can request and gain access to a specific block of information in the database and benefit from this. For future implications, a revenue model can be formed whereby the stakeholder can perform an actual transaction in exchange for the data collected by the NVWA. In this way, the requesting party obtains 100% reliable data (i.e. non-altered) and the NVWA obtains a financial reward. This revenue model is adapted from the way Nakamato links transactions in a tamper-resistant manner and prevents the double spending problem (Popovski et al., 2014).

This has also been illustrated in the case of the farmer communicating with the NVWA. Nowadays, when a farmer complies with certain regulations concerning processing and storing of manure, the farmer obtains a subsidy. In current operations, the subsidy processes are still done by 'manual' inspections on the farmer's parcel. However, now with the use of drones in combination with blockchain, this process can be fully digitised. The inspector can perform inspections with the use of the drone and check with its required payload if the farmer complies with the regulations set. The data is then transferred to the blockchain and in case a green-light is given, the farmer can get automatically receive a reward, i.e. the subsidy. This allows inspections to become fully digitised, lowering the burden on inspectors. Besides, its decentralised nature would probably decrease the delay in receiving subsidy by the farmer. Simultaneously, the data of the inspections are stored in the blockchain, making tracing back easy for future purposes of the farmer or inspection service (NVWA).

Similarly, collaboration possibilities (e.g. a consortium) arise in this way. Let's say another governmental agency desires to gain access to the data collected by the NVWA because of an incident occurrence nearby. The requesting party, who is part of the network, can now easily request and gain access to this data in a transparent and secure way. Besides, there is no need for another drone operation in the same area which reduces overall cost and time waste.

This collaboration possibility has already been referred to by multiple stakeholders in the interviews as an on-going project called Drone2Go. Their goal is to develop a network of base station from which drones can be deployed remotely and fully autonomous to respond to incidents (Weij, 2021). The involved players will share their drones hence data such that a first-responding team can act in case needed. Now the introduction of blockchain could be great aid in sharing and managing the data in a transparent and secure way, benefiting multiple organisations at once.

Furthermore, besides the various opportunities it creates for the NVWA in the field of data management, blockchain could also be of great use as a real-time logbook containing information of all active drones, what their purposes/tasks are and who is in charge. Skygrid (2020) mentions the need for a blockchain system in unmanned aviation for the integration of drones in controlled airspace. Its autonomous nature would thereby remove the burden on operators and authorities. For the NVWA, this could imply that a real-time logbook would ensure a more safe airspace. Especially when a consortium is formed, all users of the network would be able to track the active drones such that incidents can be prevented. Its accurate flight data controlled by the blockchain would hence serve as a type of traffic control, with the goal to reduce the safety risks.

Lastly, another relevant implication would be the role of blockchain as an insurance record system in case of an incident occurrence. A research by Demir, Turetken & Ferworn (2019) looks into blockchain's transparent vehicle insurance management for the case of electric and autonomous cars. An insurance record system is proposed which would act as evidence in the event of an incident. The various stakeholders such as insurance companies, drivers and lawyers would be part of the network to access the data and give a fair judgement in case of an incident. Blockchain's encrypted and immutable data storing characteristics enables insurance companies or authorities to identify the exact cause of an incident. The same can of course be implied for the case of the drone activities performed by the NVWA. If for instance a collision between two drones occurs, the data of the operation including time stamps will be available in the ledger which cannot be altered. The various stakeholders can easily identify the root cause of the incident, saving the organisation and authorities a lot of time and money.

8 Conclusion

The arrival of Industry 4.0 had enabled the boundary between the physical and digital realm to fade away. The increase in trends such as Unmanned Aerial Systems (i.e. drones) disruptively transforms industries, creating novel and arguably more efficient solutions (Esri, n.d.). The fast pacing development has however outrun the human understanding and experience of usage, imposing challenges with regards to the technical security and trust of the technology (Coetzee & Eksteen, 2011). The NVWA is one of those organisations which adopted the technology and wishes to expand their operations in various application domains. However, the lack of transparency in the current process of acquiring data by means of drones remains to be an issue. The focus must be transferred to the translation of the work process, such that a more responsible adoption rate is achieved and more application domains in the Netherlands can be enriched with the use of drones by the NVWA. Therefore, this research investigated the question: 'How to improve the work process of drone detecting services used by the NVWA such that a more responsible adoption rate is achieved?'

In this pursuit, Section 1.3 divided this question into three facets; exploring the current implementation process of the NVWA, exploring the value it creates and its barriers, and lastly the identification of the sociotechnical effects.

This research first investigated the current process of implementing drone detecting services by the NVWA. An explorative research was performed looking at both secondary as well as primary data obtained from interviews. The resulting section clearly described current applications, payload options and a visualisation of the current work process of an operation, including bottlenecks. This resulting figure gave a clear representation of how an operation looks like and bottlenecks were found in the organisation's blurring techniques, data storage techniques and safety protocol. The three relevant bottlenecks were verified by the interviewees and served as an input for the redesign.

After the current process was clearly illustrated, it was investigated how the drone detecting services by the NVWA create value and what are its barriers or disruptive threats. The most important benefits were implicitly found in the current activities and payload options of the NVWA. The drone's agile abilities are very beneficial for detecting and inspecting purposes over large areas. Faster and more accurate detection rates are achieved and due to the drone's agile abilities, areas and objects which are normally hard to identify/visualise can be easily visualised. The drone hence ensures more safe operations due to the removal of the human interaction factor. This is made possible because of its various range of payload options.

Subsequently, the resulting disruptive threats were mainly associated to privacy, data protection and ethical issues. Comparisons were made with CCTV and helicopter surveillance and existing studies by Fin et al. (2013) had shown that UAS surveillance can undermine data protection principles such as transparency, consent and rights of access. Together with the further security and safety concerns, this verifies the knowledge gap found. Furthermore a distinction between noise and visual pollution was found to be a disruptive threat by the implementation of drones.

Finally, the third sub-question was answered whereby the sociotechnical effects of the use of drone detecting services by the NVWA was investigated. The results showed correlations between the motives of usage, obstructions identified and key values to the individual stakeholder. Subsequently, it was shown how the stakeholders are linked to each other and influence the operations of the NVWA. The resulting value map led to a distinction of five key values; efficiency, safety, innovate, security, privacy and reputation. The worked out values verified the findings in the literature review in Chapter 1 and showed linkage between the found bottlenecks of Chapter 3.

The combination of the above information was used as an input for the design phase which resulted in an answer to the main research question. The bottlenecks found were related to the values safety, security and privacy which are respectively connected to the lack of transparency in the current process. A trade off of three different security techniques was performed based on set criteria such as reliability, availability and maintainability. This led to blockchain technology being the best performing security technique in this context. Blockchain technology is an innovative way of storing and sharing data and increases the whole system's security level and transparency. A form of data management by means of blockchain technology was proposed which allows the process to be more responsible. Use-cases showed that it could benefit multiple stakeholders involved and mitigate the current obstacles while enhancing the key values identified. In future projects, it could even lead to collaboration possibilities and revenue models with the users in the network, making the design generalisable.

The research concludes that blockchain technology is a promising method to improve the current work of drone detecting services used by the NVWA such that more responsible adoption rate is achieved. The redesign has shown to work in multiple use-cases and has been evaluated to be theoretically valid for usage.

8.1. Scientific Contribution

The implementation of drones is growing rapidly and multiple organisations start to adopt the technology in their current practices. The smart industry is constantly growing and digitisation is the new norm. Although this technology has passed its main developing stages, social values emerge and evolve during the development and implementation. A need for responsible innovation arose which means taking the social values into account throughout the roll-out and use of the technology. The lack of transparency in the process of implementing drones by the NVWA indicates there is a need for a more responsible design.

The research contributes knowledge to the organisation by clearly mapping the current obstructions experienced by multiple stakeholders involved and proposing where to focus on. The three phases of an operation are worked out and some vulnerabilities or bottlenecks are identified. In other words, the organisational issues are explained to facilitate a better understanding of where the redesign will focus on.

Furthermore, the research contributes to existing literature by proposing a novel technique of data management known as blockchain technology. The technology is nowadays used for digital transactions but is adapted to the case of the NVWA. Moreover, this research combines the technique with the fast-growing technology known as drones in order to come up with both a novel, useful and responsible redesign. The redesign, consisting of blockchain technology, enables to fill up the gap in research and potentially benefits multiple stakeholders making use of the service. The organisation is educated with the use of the technology in different use-cases such that its design and motive for usage is made clear. Furthermore a bridge is made between on-going projects whereby a consortium is highly favored. This clearly shows the technology can be generalised and should be looked into by future researchers.

8.2. Societal Contribution

This research contributes to society due to its generalisable nature. As said, multiple organisations making use of drones could implement this system hence make their operations more responsible. In this way, the system is more transparent to others and thanks to its decentralised structure, it is more secure against cybercrime.

Moreover, organisations could form a consortium whereby they can share data collected by drones and therefore benefit multiple users at once. Blockchain allows transactions or data transfers to be safe and secure with full transparency among the users in the network. The preliminary design in this research can be used as a guideline for the development of a future drone network e.g. Drone2Go. The obstructions, involved players and their values are clearly linked to the redesign which can be adapted to multiple cases, hence contributing to society.

Furthermore, making the implementation of drones more responsible by taking social values into account is highly favored among the society. Key values such as safety, privacy and security are implemented such that drone-use can achieve a high acceptance level. Favorably, a similar trust level as the adoption of CCTV or satellite surveillance is achieved. Although blockchain would lead to 'disruptive' changes in the current process, its characteristics compared to regular databases are promising and would mitigate multiple (societal) issues addressed.

8.3. Relevance to Study Programme

With the study programme Management of Technology (MOT), the student learns to explore and understand technology as a corporate resource.

In other words, MOT graduates have learned to discover how companies can use technology to design and develop products and services that help improve business productivity, customer satisfaction, competitiveness and profitability. Moreover, graduates are able to analyse the commercial impact of technologies and can implement these in an organisational context within the organisation or firm. Relating this the research, both technological as well as organisational aspects were taken into account which matches with the type of research of a Management of Technology student.

Actors and factors that affect the further implementation of drones were analysed which required the use of both technical and strategical knowledge such that an understandable output was given to the organisation. Moreover, blockchain technology was discovered to be a potential solution and a preliminary design was showcased. A responsible redesign was proposed including use-cases which showed how the organisation benefits from the insights retrieved by the student. A novel solution was hence given including critical insights of why this would be a suitable resource of use. A technological yet managerial approach was used, which is perfectly linked to a regular research of the study Management of Technology.

8.4. Future Research & Reflection

Integration of blockchain in the field of drone detecting services is an exciting and novel field of research. Due to its novelty, there remain quite some limitations to exist which could serve as an input for potential future research.

First of all, an analysis of the reliability and implementation of the responsible redesign within the organisation should be done. This study would fully validate the proposed redesign and hence be looked into further for organisations. Of course the actual implementation would be unrealistic however one could look at the first steps to be taken. Think about setting up the smart contracts, the nodes and encryption tools. This would be an interesting first step towards the use of blockchain and drones by the NVWA.

Simultaneously, looking into the on-going project called Drone2Go whereby a consortium is formed with all stakeholders and benefiting parties, would be of great value. This study was done in the case of the NVWA, however future projects could go one step further and look at the collaboration between the five first responders; Rijkswaterstaat, Fire Department, Police Department, ILT and the NVWA. The current research started by looking at the implementation process of this project however came to a rough end due to varying legal issues experienced. The various operators or responders have different authorizations which makes the construction of one protocol difficult. Now with the final redesign ready for the case of the NVWA, more insights can be obtained for future research. In fact, the Head of Department Trade & Digital Surveillance was so excited about the design that he wanted to showcase this during a presentation with the involved parties of Drone2Go. This verifies the usefulness of the idea hence the usefulness of future research.

Lastly, future research should be done in the Dutch legal framework concerning drone-use. Many stakeholders indicated this to be a main obstruction and is hard to change. Reflecting back to this research, quite some difficulties were experienced in finding out how the Dutch legal framework influences the adoption of drones. Its complexity and highly dynamic nature made it hard to draw conclusions. Besides, there exist many exceptions in the legislation which made it even harder. Since law is out of the scope of this research, it would be interesting to look at the critical points of the Dutch legal framework which delays the further expansion and usage of drones in agriculture.

On another note, a social study could be conducted to see what would happen if blockchain was implemented and transparency and security are no longer an issue in the process. Would the use of nationwide drones in different contexts become as socially accepted as the use of CCTV and satellite surveillance? This would be an interesting subject to be found out in the future.

References

Alladi, T., Chamola, V., Sahu, N., & Guizani, M. (2020). Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications*, *23*, 100249.

Ashford, W. (2019). *Encryption adoption driven by new tech and compliance.* Retrieved 2021-07-22, from `https://www.computerweekly.com/news/252460545/Encryption-adoption-driven-by-new-tech-and-compliance`

Authy. (n.d.). *What is two-factor authentication (2fa)?* Retrieved 2021-07-22, from `https://authy.com/what-is-2fa/`

Aydin, B. (2019). Public acceptance of drones: Knowledge, attitudes, and practice. *Technology in society*, *59*, 101180.

Bassi, E., Bloise, N., Dirutigliano, J., Fici, G. P., Pagallo, U., Primatesta, S., & Quagliotti, F. (2019). The design of gdpr-abiding drones through flight operation maps: A win–win approach to data protection, aerospace engineering, and risk management. *Minds and Machines*, *29*(4), 579–601.

BBC. (2017). *Dji drones to gain privacy mode after us army ban.* Retrieved 2021-06-02, from `https://www.bbc.com/news/technology-40935860`

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the internet of things (iot): A systematic review of the benefits and risks of iot adoption by organizations. *International Journal of Information Management*, *51*, 101952.

Cawthorne, D., & Robbins-van Wynsberghe, A. (2020). An ethical framework for the design, development, implementation, and assessment of drones used in public healthcare. *Science and Engineering Ethics*, *26*(5), 2867–2891.

Chen, C.Y., & Klette, R. (1999). Image stitching—comparisons and new techniques. In *International conference on computer analysis of images and patterns* (pp. 615–622).

Cheung, S.-C., Venkatesh, M. V., Paruchuri, J. K., Zhao, J., & Nguyen, T. (2009). Protecting and managing privacy information in video surveillance systems. In *Protecting privacy in video surveillance* (pp. 11–33). Springer.

Choi, S.-C., Sung, N.-M., Park, J.-H., Ahn, I.-Y., & Kim, J. (2017). Enabling drone as a service: Onem2m-based uav/drone management system. In *2017 ninth international conference on ubiquitous and future networks (icufn)* (pp. 18–20).

Christensen, C., Raynor, M. E., & McDonald, R. (2013). *Disruptive innovation*. Harvard Business Review.

Christian, A. W., & Cabell, R. (2017). Initial investigation into the psychoacoustic properties of small unmanned aerial system noise. In *23rd aiaa/ceas aeroacoustics conference* (p. 4051).

Cimpanu, C. (2019). *Microsoft: Using multi-factor authentication blocks 99.9% of account hacks.* Retrieved 2021-07-22, from `https://www.zdnet.com/article/microsoft-using-multi-factor-authentication-blocks-99-9-of-account-hacks/`

Coco-Stotts, K. (2020). *Vulnerabilities of multi-factor authentication for remote working.* Retrieved 2021-07-22, from `https://jumpcloud.com/blog/vulnerabilities-mfa-remote-work`

Coetzee, L., & Eksteen, J. (2011). The internet of things-promise for the future? an introduction. In *2011 ist-africa conference proceedings* (pp. 1–9).

Corrigan, F. (2020). *12 top collision avoidance drones and obstacle detection explained.* Retrieved 2021-04-14, from `https://www.dronezon.com/learn-about-drones-quadcopters/top-drones-with-obstacle-detection-collision-avoidance-sensors-explained/`

Custers, B. H. M., Oerlemans, J.-J., & Vergouw, S. (2015). *Het gebruik van drones*. Boom Lemma.

Customdrone. (n.d.). *Wat kunt u zien met een lidar drone? | custom us | customdrone.* Retrieved 2021-04-10, from `https://www.customdrone.com/kennisbank/lidar-scan-drone`

Davies, A. (n.d.). *How much does it cost to build a blockchain project?* Retrieved 2021-08-15, from `https://www.devteam.space/blog/how-much-does-it-cost-to-build-a-blockchain-project/`

de Graaff, T. (2020). *Pilotproject: drone-inspecties in attractieparken.* Retrieved 2021-04-08, from `https://dutchmobilityinnovations.com/spaces/1191/drone2go/articles/news/36294/pilotproject-drone-inspecties-in-attractieparken`

de Jager, W. (2020). *Drones binnen de gemeente* (Tech. Rep.). n.a.: VNG Realisatie.

Demir, M., Turetken, O., & Ferworn, A. (2019). Blockchain based transparent vehicle insurance management. In *2019 sixth international conference on software defined systems (sds)* (pp. 213–220).

de Reuver, M. (2019). *Mot2312 2019-2020 lecture 3.1. data collection operationalization.* University Lecture.

Doubleday, K. (2018). *Blockchain immutability — why does it matter?* Retrieved 2021-06-14, from `https://medium.com/fluree/immutability-and-the-enterprise-an-immense-value-proposition-98cd3bf900b1`

Dugdale, S. J., Kelleher, C. A., Malcolm, I. A., Caldwell, S., & Hannah, D. M. (2019). Assessing the potential of drone-based thermal infrared imagery for quantifying river temperature heterogeneity. *Hydrological Processes*, *33*(7), 1152–1163.

Esri. (n.d.). *What is gis?* Retrieved 2021-05-10, from `https://www.esri.com/en-us/what-is-gis/overview`

European Union Aviation Safety Agency (EASA). (2021). *Study on the societal acceptance of urban air mobility in europe.*

Fernández-Caramés, T. M., Blanco-Novoa, O., Froiz-Míguez, I., & Fraga-Lamas, P. (2019). Towards an autonomous industry 4.0 warehouse: A uav and blockchain-based system for inventory and traceability applications in big data-driven supply chain management. *Sensors*, *19*(10), 2394.

Filcak, R., Povazan, R., & Viaud, V. (2020). *Delivery drones and the environment* (Tech. Rep.). n.a.: European Environment Agency.

Finn, R. L., & Wright, D. (2016). Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organisations. *Computer Law & Security Review*, *32*(4), 577–586.

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. In *European data protection: coming of age* (pp. 3–32). Springer.

Freeman, R. E. (2015). Stakeholder theory. *Wiley encyclopedia of management*, 1–6.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018, 02). Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet*, *10*, 20. doi: 10.3390/fi10020020

Griffiths, F., & Ooi, M. (2018). The fourth industrial revolution-industry 4.0 and iot [trends in future i&m]. *IEEE Instrumentation & Measurement Magazine*, *21*(6), 29–43.

Gurl, E. (2017). Swot analysis: A theoretical review.

Herrick, S. (2017). *Rgb versus nir: Which sensor is better for measuring crop health?* Retrieved 2021-04-14, from `https://botlink.com/blog/rgb-versus-nir-which-sensor-is-better-for-measuring-crop-health`

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian journal of information systems*, *19*(2), 4.

Higginson, M., Nadeau, M.-C., & Rajgopal, K. (2019). Blockchain's occam problem. *McKinsey and Company*.

Hoelscher, J. (2014, 02). Diffused art and diffracted objecthood: Painting in the distributed field..

Insider Intelligence. (2021). *Future of drones: Applications & uses of drone technology in 2021.* Retrieved 2021-06-09, from https://www.businessinsider.com/drone-technology-uses-applications?international=true&r=US&IR=T

Iredale, G. (2020). *Blockchain vs database: Understanding the difference.* Retrieved 2021-06-17, from https://101blockchains.com/blockchain-vs-database-the-difference/

Jafary, B., Bhattacharya, S., Nafreen, M., Yuan, S., Zhou, J., Wu, L., … others (2019). *The application of unmanned aerial systems in surface transportation–volume ii-f: Drone cyber security: Assurance methods and standards* (Tech. Rep.). n.a.: University of Massachusetts Dartmouth.

Jenkins, D., & Vasigh, B. (2013). *The economic impact of unmanned aircraft systems integration in the united states*. Association for Unmanned Vehicle Systems International (AUVSI).

Khan, P. W., Byun, Y.-C., & Park, N. (2020). A data verification system for cctv surveillance cameras using blockchain technology in smart cities. *Electronics*, *9*(3), 484.

Kreuter, M. W., De Rosa, C., Howze, E. H., & Baldwin, G. T. (2004). Understanding wicked problems: a key to advancing environmental health promotion. *Health education & behavior*, *31*(4), 441–454.

la Cour-Harbo, A. (2019, 02). Quantifying ground impact fatality rate for small unmanned aircraft. *Journal of Intelligent and Robotic Systems*, *93*. doi: 10.1007/s10846-018-0853-1

Lastovetska, A. (2021). *Blockchain architecture basics: Components, structure, benefits & creation.* Retrieved 2021-06-16, from https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of family medicine and primary care*, *4*(3), 324.

Levenson, M. (2021). *1,500 eggs were waiting to hatch. then a drone crashed.* Retrieved 2021-06-08, from https://www.nytimes.com/2021/06/04/us/elegant-tern-eggs-drone-crash-california.html

MarketsandMarkets. (2020). *Encryption software market by component (software and services), application (disk encryption, file/folder encryption, communication encryption, cloud encryption), deployment mode, enterprise size, vertical, and region - global forecast to 2025.* Retrieved 2021-22-07, from https://www.marketsandmarkets.com/Market-Reports/encryption-software-market-227254588.html

Matthews, K. (2020). *7 advantages of using encryption technology for data protection.* Retrieved 2021-07-22, from https://www.smartdatacollective.com/5-advantages-using-encryption-technology-data-protection/

Migdall, S., Klug, P., Denis, A., & Bach, H. (2012). The additional value of hyperspectral data for smart farming. In *2012 ieee international geoscience and remote sensing symposium* (pp. 7329–7332).

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad hoc networks*, *10*(7), 1497–1516.

Momont, A. (2014). Ambulance drone. *Delft University of Technology*.

Natuur & Milieu. (2018). *"met nieuwe technieken kunnen we ons werk nog beter doen".* Retrieved 2021-06-02, from https://magazines.nvwa.nl/jaarverslag/2018/01/met-nieuwe-technieken-kunnen-we-ons-werk-nog-beter-doen

NVWA. (n.d.). *About us | nvwa.* Retrieved 2021-04-10, from https://english.nvwa.nl/

NVWA. (2021). *Fundement ai drones/applicaties.* Powerpoint.

OSS Encryption. (2016). *The three methods of database encryption.* Retrieved 2021-07-22, from https://mydiamo.com/the-three-methods-of-database-encryption/

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45–77.

Pesch, U., & Werker, C. (2019). *Technology dynamics (mot1412).* University Reader.

Poplawska, J., Labib, A., Reed, D. M., & Ishizaka, A. (2015). Stakeholder profile definition and salience measurement with fuzzy logic and visual analytics applied to corporate social responsibility case study. *Journal of Cleaner Production*, *105*, 103–115.

Popovski, L., Soussou, G., & Webb, P. (2014). A brief history of blockchain. *Patterson Belknap Webb & Tyler, New York, NY, USA, Tech. Rep*.

Press Release. (2006). *The cost of implementing multi-factor authentication.* Retrieved 2021-07-22, from https://www.24-7pressrelease.com/press-release/10729/the-cost-of-implementing-multi-factor-authentication#:~:text=The%20total%20cost%20of%20ownership%20for%20implementing%20a%20Hardware%20Token,took%20the%20longest%20to%20implement.

Radovic, M. (2020). *Global drone outlook 2020: What's on the agenda.* Retrieved 2021-05-14, from https://droneii.com/global-drone-outlook-2020

Rijksoverheid. (n.d.-a). *Human environment and transport inspectorate.* Retrieved 2021-05-17, from https://ilent.nl/

Rijksoverheid. (n.d.-b). *Ministry of infrastructure and water management | organisation.* Retrieved 2021-05-17, from https://www.government.nl/ministries/ministry-of-infrastructure-and-water-management/organisation

Russel, J. (2019). *Facebook is reportedly testing solar-powered internet drones again — this time with airbus.* Retrieved 2021-04-14, from https://techcrunch.com/2019/01/21/facebook-airbus-solar-drones-internet-program/

RVO. (n.d.). *Wat doet rvo?* Retrieved 2021-08-15, from https://www.rvo.nl/over-ons/werken-bij-rijksdienst-voor-ondernemend-nederland/wat-doet-rvo-0

Skalex. (n.d.). *Transform your business with blockchain technology.* Retrieved 2021-06-13, from https://www.skalex.io/support/blockchain/blockchain-technology/

Spamlaws. (n.d.). *Database security issues: Database security problems and how to avoid them.* Retrieved 2021-07-22, from https://www.spamlaws.com/database-security-issues.html

Spieksma, M., & Voss, D. (2020). *Complotdenken over 5g en de pandemie: hoe een twitterstorm zendmasten kan vellen.* Retrieved 2021-05-29, from https://www.ad.nl/binnenland/complotdenken-over-5g-en-de-pandemie-hoe-een-twitterstorm-zendmasten-kan-vellen~ae8c19ed/

T&A Survey. (n.d.). *Grondradar*.* Retrieved 2021-04-14, from https://www.ta-survey.nl/page/324/NL/drone-onderzoek/technieken/grondradar

Taebi, B., Correlje, A., Cuppen, E., Dignum, M., & Pesch, U. (2014). Responsible innovation as an endorsement of public values: The need for interdisciplinary research. *Journal of Responsible Innovation*, *1*(1), 118–124.

Takyar, A. (n.d.). *How to determine the cost of blockchain implementation?* Retrieved 2021-06-16, from https://www.leewayhertz.com/cost-of-blockchain-implementation/

Tapscott, D., & Tapscott, A. (2017). How blockchain will change organizations. *MIT Sloan Management Review*, *58*(2), 10.

Tarasenko, E. (2019). *How much does it cost of blockchain implementation.* Retrieved 2021-08-15, from `https://merehead.com/blog/how-much-does-it-cost-of-blockchain-implementation/`

Valavanis, K. P., & Vachtsevanos, G. J. (2015). *Handbook of unmanned aerial vehicles* (Vol. 1). Springer.

Von Schomberg, R., et al. (2013). A vision of responsible research and innovation. *Responsible innovation: Managing the responsible emergence of science and innovation in society*, 51–74.

Weij, M. (2021). *Memo: Drone2go sprint 6.* (Unpublished Memo)

Williams, M., & Moser, T. (2019). The art of coding and thematic exploration in qualitative research. *International Management Review*, *15*(1), 45–55.

Zorz, Z. (2016). *Icarus takes control of drones by impersonating their operators.* Retrieved 2021-06-08, from `https://www.helpnetsecurity.com/2016/10/27/control-drones-icarus/`

A
Interviews

A.1. Explorative Mapping

P1: Specialist Risk & Crisis Management / Strategic Advisor

1. Could you introduce yourself?

As a quartermaster of the DO-IT platform, a platform for drones linked to detection, investigation, incident control and supervision, together with the Public Prosecution Service, NVWA, IFV, the National Police, Department of Waterways and Public Works, ILT Aerosensing and Defense, I am exploring the possibilities to increase the chain collaboration concerning innovation projects with drones and remote sensing, covering a number of common themes such as data management, privacy and ethics, political lobbying, business development (procurement, tendering, IP), education and training, management.

2. What is the current biggest obstacle/problem for the implementation of drones and sharing of resources/data?

You can distinguish between three different obstacles currently in the Netherlands. The first and most common known is the Dutch legal framework. Although in January this has been adjusted, the current legal framework remains to be rather conservative and strict. Especially the regulations concerning autonomous flying drones, for both commercial and recreational usage, remain to be an issue for sensitive obstacle.

On the other side, many drone projects and developments remain to be sitting in the prototyping phase. Resources such as money remain to be an issue to further develop the product hence the obstacle for implementation in certain application domains. This goes hand in hand with the last point, which is the insecurity factor. If the government is not convinced, the procurement law leads to financial uncertainty. Companies which have invested money and time hence experience uncertainty about governmental support.

Adding up, there is a need for a certain importance of protocols of action. Transparency or traceability must be present such that inspectors can perform, and trace back, their tasks. Often there is too much focus on the technology and too little in the translation to the work process. Tracing back is an important factor to be considered here.

3. How do you think this can be improved in the short term?

Improving a legal framework is always hard. The Netherlands is known to be conservative hence difficult to change. Points to be improved in the short term are related to the last points mentioned. If we focus more on translating the work process by being transparent and allowing traceability, a higher level of acceptance might be achieved. Compare it with 10 years ago when CCTV arose. Huge societal fear existed, e.g. unethical nor legally possible. The same holds for drone-use now. Perhaps we can adapt it to the current situation and learn from our 'mistakes'.

4. Looking at the situation now, what are the next steps to solve the problems discussed?

Conduct successful experiments in practice. Dare to set a goal and work your way to it. Make up a story such that concrete projects can show examples of the service's added value. In this case, it exists of 2 vessels; data management and legal feasibility. If these are connected to each other, together with a opportunistic goal, we can slowly move to the desired end goal. We need to anchor this idea into our daily life, hence need early adopters/leaders with courage and a motive to invest in the innovation.

P2: Specialist Remote Sensing & Data Acquisition / Senior Inspector (NVWA)

1. Could you introduce yourself?

I am head of the team Remote Sensing & Data Acquisition which is part of the department Trade & Digital Surveillance at the NVWA. I started the department together with one colleague back in 2017 which has grown to a total number of 14 now. Our team has been innovating and experimenting with drones to improve the NVWA's current surveillance techniques. We now use drones for detecting, surveillance, and monitoring purposes. My ultimate goal is to share our drone techniques with other parties such that a nationwide access to the drones is achieved, and more efficient solutions are obtained.

2. What is the current biggest obstacle/problem for the implementation of drones and sharing of resources/data?

For us the main obstacle is related to the translating part in the process. More specifically, the protocol of actions in the process. The timeframe between acquiring data and translating such that useful results are obtained has proven to be slow and uncoordinated. Stitching, or the translation of 'rough data', is often slow and lacks protocol. Also, most of the data management is still done by hand without using (cloud) servers et cetera. This stresses a lack of traceability which should be tackled. Ultimately, if the process of translating data to useful data for inspectors is done faster, data sharing could benefit multiple parties.

Besides, in some cases data can be privacy sensitive which is now blurred by hand. Bottlenecks hence exist in determining if the data is useful, contains no privacy sensitive information and thus can be shared.

3. How do you think this can be improved in the short term?

As said, optimising this process of translating rough data to useful data would proof this solution is more efficient and faster than the conventional (manual) method used during inspections. If this is proven to be faster and more efficient, this method can be standardised in the long term and more promising experiments can be performed.

4. Looking at the situation now, what are the next steps to solve the problems discussed?

Simple said, keep experimenting and work on a protocol of action. If this process is transparent and standardised, 3rd parties such as conventional inspectors and the government may be convinced and a faster adoption rate will be achieved.

P3: AI Specialist / Data Engineer (NVWA)

1. Could you introduce yourself?

I am part of the team Remote Sensing & Data Acquisition of the department Trade & Digital Surveillance at the NVWA. My responsibilities lay with all the AI developments such as image recognition in various application domains. More specifically, I build models and train algorithms for the identification and visualization of certain species or phenomena, e.g. Asian Tiger Mosquito or the Amazon parrots.

2. So what does the current work process of such an operation look like?

The first step is to train the algorithm. This is done by collecting big amounts of data in various conditions. As an example, for illegal fyke detection we train the algorithm by making approximately 6,000 pictures in various external conditions, e.g. sunny day, rainy, cloudy water, different light angles etc. The more data you collect, the better trained hence more precise it will be in practice.

The next step is to make a flight plan, determine the necessary payload and start the operation. The drone collect data by taking a picture every second. The collected data is saved on the drone's internal SD card and will be translated after the operation by the use of AI software installed on certain laptops in the office. The software, based on its training sessions, translates the data and identifies and indicates possible fyke positions on a visual map. This is then communicated to an inspector which can then conduct its inspections based on the indicated 'high-risk of illegal fyke' coordinates.

3. What is the current biggest obstacle/problem for the implementation of drones and sharing of resources/data?

The collected data is now simply saved on the hard-drive of a laptop in the office of the NVWA. Favourably, this data is stored on a server/cloud such that multiple individuals can get access to this. This however remains an issue due to the GDPR and American companies being responsible for the servers.

Besides there are multiple applications required for an operation to take place. For instance there is an app for checking weather conditions, checking no-fly zones, requesting a permit, et cetera. Apart from this, most data analysis is done by hand. For instance data stitching, the process of 'stitching' images to each other to get a visual map, and blurring personal information is done manually which takes quite some time during an operation. This could lead to delays, making the process less efficient hence can be seen as an obstacle.

4. How do you think this can be improved in the short term?

Favourably, data will be stored in cloud servers such that multiple individuals can get access and perform algorithms to analyse the data in real-time. Having a server however requires a protocol of action in terms of handling the data in a safe and secure way.

Also, uniformity in all the applications necessary for an operation would be beneficial. Translating and transferring all this information in one platform would fasten the process, hence increase efficiency.

A.2. Stakeholder Analysis

S1: Lector Advanced Forensic Technology (Saxion)

1. Could you introduce yourself?

I am doing a joint professorship together with the Dutch Police department and Saxion. I am involved in four continuous lines of research whereby we use innovative technologies for investigations. The first line of research concerns nanoforensics whereby we make use of nanotechnology to detect and remotely analyse. The second line concerns forensic robotics whereby we make use of flying or non-flying robotics during our investigating operations. The third line concerns data science and crime where we are busy with constructing algorithms and machine-learning. The last one consists of silent witness and coldcase.

2. What are your organisation's responsibilities?

I am a lector and work with the Police department. My responsibilities lay with doing research in those four fields and of course implement where possible in investigating activities.

3. What is your institute's role in a drone operation of the NVWA?

Our role is very dependent. Only recently we have been able to make use of NVWA's drone techniques to see if this technique can be used for our operations. For instance the drone detecting service, able to identify and localize cadavers can be used in a similar domain but then for human bodies (hidden graves). The same holds for the NVWA's sniffer drones; this can be used for the detection of narcotics. Another project we work in collaboration with the NVWA is called Drone2Go whereby we want to combine the drone techniques and data such that first responders can make use of it. So we are a collaborating party whereby we share the knowledge and resources for various crime scene applications.

4. What values weigh the most for you?

For us the most important value is faster and more efficient detection in investigating activities. The various sensors available can allow first responders to get faster results and work more effectively. Besides, the implementation of robotics allow a lower level of human interaction hence increases safety (in some situations).

5. In terms of innovation, what is your ultimate goal?

Our ultimate goal is to form a consortium with all first responding teams. The construction of one team can then make use of the drones and data and share this among each other such that faster results are obtained. Now, all agencies have their own drones and training. Depending on the situation and which party is first present, data is collected but not shared to the others. This often leads to time being waste hence an inefficient process. This would be tackled if a consortium is being set up.

6. What are the current biggest obstructions for reaching this goal?

There remains a lack of one operational support team responsible for the drone operations. In many situations, the operation remains time-consuming and potentially dangerous. There is not yet one team responsible for the implementation of drones; all parties have their own drones and protocols. A cross-disciplinary approach must be implemented such that the first responding work field can benefit from this. When there is an incident, the data can then be shared with them such that they can work faster *and more efficient.*

S2: Technical/Accountable Manager ILT (Aerosensing dept.)

1. Could you introduce yourself?

I am since 2013 working at ILT and started a drone team called Aerosensing within ILT with my colleague in January 2020. I am the technical manager and temporary accountable manager of the team which makes me responsible for technical inspections and the team itself. We have 6 fixed pilots/inspectors, 8 part timers and 1 project leader.

2. What are your organisation's responsibilities?

We are an inspection service with around 1200 employees divided over 170 departments. ILT has a supervising purpose in varying legislations such as hazardous substances in water, air or on land. Moreover we perform inspections on freight transport, taxi transport, environmental and more. We also supervise contractors working on important Dutch infrastructure such as the Afsluitdijk, i.e. to see if the company is working in accordance with its permits. Besides we have a major licensing branch in aviation; so to determine if they are allowed to fly and check permits et cetera.

3. What is your organisation's role in a drone operation of the NVWA?

We don't do many operations together with the NVWA. In the past, we have had some cases where we shared our resources (drones or flights) with each other. Our main role is to be found in the preparation phase. We work together on the pilot training, setting up the flight company, having the right certificates and permits and other. More specifically we work on arranging the drone team. ILT has a supervising task on all parties with permits to conduct drone operations, including the NVWA. I personally work on a separate branche of ILT called Areosensing which is similar to the NVWA. ILT hence also supervises our team. Every exemption and permit must be paid to the ILT. For us it is however hard to get these permits since we fly under the name ILT. This comes with a great responsibility hence face a great risk of reputation damage, in case something goes wrong.

4. What values weigh the most for you?

I know that the NVWA's drone team has a vision to supply all inspectors with drones. ILT on the other hand is often active in industrial areas where flying is not allowed with light drones. This requires more trained pilots with a ROC license. ILT does not have the vision yet to supply all inspectors with this license and drones. The implementation of drones merely started as a hobby and grew to a small team within ILT. We look for innovating inspection methods which is why it is decided to spend 70 % of the working time on innovation. Apart from that, ILT values safety extremely high. I like to compare us to the brightest boy or girl in class. As said before, ILT operations are checked more neatly than others due to its perceptive risk of reputation damage.

5. What are the current biggest obstructions for reaching this goal?

In one word; the Dutch Government. The hierarchical structure of the organisation in combination with the Dutch government makes innovating very hard. Many are sceptical and don't want to take responsibility. The Ministry decided how much money we get. The lack of knowledge and trust has led to a low budget in the past hence makes growing difficult for us. Low budget due to lack of trust and responsibility by the Dutch Government is thus critical.

S3: Accountable Manager Rijkswaterstaat (Drone Team)

1. Could you introduce yourself?

I am accountable manager of the drone team of the Rijkswaterstaat. This role makes me responsible of the flight operations within the Rijkswaterstaat. I do this part-time because I also work as service delivery agent, hydroglogist and at the central information provision office. This makes me responsible for all IT within our organisation. The idea of the drone team started in 2016 with only a small group of LIGHT pilots. After working ourselves bottom-up, we slowly expanded to a professional organisation with more trained pilots embedded within the Rijkswaterstaat.

2. What are your organisation's responsibilities?

The Rijkswaterstaat itself is an executive agency working under the policy set by the Ministry of Infrastructure and Water Management in the Netherlands. We are mainly responsible for incident control and prevention. So we look at the design, construction, management and maintenance of the main infrastructure in the Netherlands, but also of course the waterway network and systems. Now our drone team is able to recognize van visualize incidents on an ad-hoc basis. As a first-responding team we fly to an incident such as an oil leakage on the open water or any other incidents in traffic, and respond fast such that mitigating measures can be taken. The duty officer gives out an order and one of our drone pilots acts fast with the purpose to control the situation and prevent further damage by mapping the situation. Please note we only work on ad-hoc basis, meaning that operations which can be planned are often carried out by other organisations such as the NVWA or ILT. In this way we help each other and divide the activities.

3. What is your organisation's role in a drone operation of the NVWA?

So similar to the NVWA, we carry out drone operations. Difference is we do not enforce nor perform inspections planned beforehand. However we do help each other in an advising way. Rijkswaterstaat was the first governmental party, apart from the army, which made use of the drone technologies. We have a big IT service hence a lot of resources and knowledge in this field. This makes us the more experienced party and leader in tooling. We therefore help and collaborate with parties such as the NVWA and ILT with their trainings. We set the base and now have a lot of experienced pilots in the field. Furthermore, together with the ILT and NVWA, in some cases we share our resources and of course flight operations where possible. In this way we can fly more efficient and benefit multiple parties at once.

4. What values weigh the most for you?

For the Rijkswaterstaat the main goal is damage control. We value this the most which is why we work on ad-hoc basis. Of course this goes hand in hand with safety; the urge of incident control and prevention where possible. On the other hand we value our reputation very much. Since we are one of the pioneers working as a drone team for the government, we have a high responsibility and risk of reputation damage. Simple said, if something goes wrong and the media takes notice of this, we will have to start all the way from the beginning again. The trust in us as one of the leading drone operators will be lost and will take years to gain back. The implementation of drones remains to depend on the public acceptance hence must be done carefully. One mistake and it's all over.

5. What are the current biggest obstructions for reaching this goal?

As just said, public acceptance remains an issue. Although we do most of our operations on the open water or in non-civil environments, we must be careful. If one of our drones unintended collects and shares privacy sensitive information or in the extreme case crashes into someone's house or worse, public acceptance will be damaged heavily. The latter is ought to happen if we constantly increase our pilots on a quantitative base in stead of qualitative. Lack of expertise increases the chance of accidents hence must be prevented. This matches why we are reluctant in performing enforcement activities with the drones. This can only be done if there is full public acceptance, which might take years from now on (if no drone scandals/accidents happen upcoming years).

Lastly, the legal framework remains an issue. The Ministry is responsible for our budget and is keen to invest in our drone operations. They are also responsible for the legal framework hence limit our services. There is still a debate about if the Ministry is going to follow the regulations set by European Union (EASA) or the State Aircraft regulations in the Netherlands. We are therefore very dependent on what they will choose in order for us to innovate and expand.

S4: Operational Specialist Dutch Police Department

1. Could you introduce yourself?

I am an operational specialist within the Dutch Police Department. With this I am responsible for the innovations within the Police which connects various other institutes such as the Fire Department, Rijkswaterstaat and other knowledge institutions. Besides I am also an operational duty officer and work on the investigation of cyber attacks.

2. What is your organisation's role in a drone operation of the NVWA?

Well our role is varying and has three perspectives. The first one is of course enforcement. Together with ILT, we are an enforing instance so we make sure the drone operators in the Netherlands obey the law. I do need to stress out that ILT is merely responsible for enforcing the aviation regulations. So to check if operators such as the NVWA have the right certificates and permits. We only do enforcement if operators are seriously breaking the law with their drones which happens almost never.

The other perspective has to do with the safety of the drone operators. More specifically, the police has a role in ensuring the safety of the drone operators of the NVWA, in case there is a risk of violence. Think about inspections for manure fraud; farmers or civilians can show aggressive behavior and do damage to the equipment or team members of the drone team. This is where the police takes its role, to ensure the safety of the team.

The third perspective has to do with mutual resources and investigations. If both parties are working in the same area of interest, resources such as data and drones are shared. This simply saves time and helps both parties. Please note that in some cases, due to sensitive data, the Police Department is not allowed to share this data with the NVWA. This has to be filtered out or is simply not shareable in that case.

3. What values weigh the most for you?

For the Dutch Police, safety is always issue number 1. We are here to ensure the safety of the people and hence make sure the law is enforced. However from the point of view as a specialist, innovative developments within the Dutch Police Department weigh a lot. A more stable implementation drones *within the various instances of the Police is desired. The implementation of drones for crime scene investigations would allow a faster and more efficient detection rate. Moreover, there are some public order issues which we would like to tackle. Think about the expansion of our pilot teams for events, demonstrations et cetera. So again, the standardization of implementing and to make it a regular tool of use, has a high value for us. This brings me to the project Drone2Go whereby we would like all first responding teams to work together by means of autonomous drones. The collaboration part, hence sharing of resources such as the drone and its collected data, allows a faster actions by first responding teams and adds great value to public safety. As you might know, we are currently active in conducting experiments with this team and achieved promising results. However, while innovating we must realize we play a big role in the Netherlands and hence have a great responsibility, and reputation. This hence brings me back to the value safety. While the opinions about innovations such as drones might vary among the individuals working for the Dutch Police Department, safety remains the highest weighing value.*

4. What are the current biggest obstructions for reaching this goal?

The first issue has to do with financing the resources required. The equipment, training and certificates come with great cost hence is an obstruction for getting a more stable drone implementation. Although we have enough budget for current operations, this remains a limiting factor for further expansion. On the other hand, the implementation of a mutual drone network has some legal issues which have to be tackled. Think about how to share the data among all players, GDPR and privacy issues. The regulations for this remain to be strict or unclear hence makes this an obstruction. This brings me to the last point which has to do with the robustness of the technology. The safety and trustworthiness is not optimal yet which have to be worked on. This will take some years to build before most parties, such as governmental instances, are fully convinced.

S5: Owner Metal Recycling & Barrel Rental (Outsider)

1. Could you introduce yourself?

I am the current owner of a family business in metal recycling and barrel import/export. We exist for almost 100 years and I am the responsible owner since 1990. Basically our main activities consists of renting and selling new and used barrels, ranging from steel barrels to IBC containers (bigger variant for mainly liquids). Apart from that, people can recycle their scrape metals (devices and machines) at our company.

2. How often do you experience inspections by governmental instances?

Not that often. I would say around twice a year I get a letter of the environmental service whereby they announce an inspection. Often one or two inspectors come across and I show them around the property and let them do their work. Sometimes they also come unannounced which can be a pain in case we just received a load of used barrels which we must clean. This makes the work floor dirty and is a bad representative of our regular work conditions.

3. Have you heard about governmental drone technologies used for inspections before?

I've seen some recreational drones before and of course have seen drones in movies however never seen them used during inspections here. I know the military is using drones and robotics for their operations but I haven't touched nor seen a governmental drone before.

4. Parties like the NVWA and Rijkswaterstaat use drone detecting services for supervision and inspections. Would you be open for an inspection performed by a drone on your terrain?
Well I don't have very much property to inspect so I am assuming this won't be necessary for my case. However, in case it would be useful, it depends. Since it is very new to me that they use a drone for such an operation, I am not sure about it. I understand the ease of the fast drones and that it saves time and money, however I wouldn't want a camera flying over my property without me knowing what it captures. Of course I have nothing to hide, but I would like to have some control over an inspection and keep my personal information save. Also, how do I know if the drone is actually from the government? A drone cannot legitimize itself while an inspector can. Also, how safe is such a drone for my machinery and personnel? What if my personnel gets recorded without their permission? Also, what if my machinery gets damaged by a mistake of a drone pilot. I think this is not worth it in my case hence would be resistant against such an inspection.

5. What would make you change your mind?
Well as said, I think I won't be needing drones for inspections for my relatively small property. However to answer your question; if a drone can legitimize itself and show me what it has done and seen I might be more flexible. I first what it is to be inspected, who is inspecting and when. Also I want to know where this data goes to and who is in charge. Also things like insurance and the removal of personal information must be covered beforehand. If this is clear to me and the drone is clearly from the government, it would be an interesting solution. For now and in my case however I think it is not necessary.

A.3. Evaluative Interviews

E1: Specialist Remote Sensing & Data Acquisition / Senior Inspector (NVWA)

1. Is it clear how blockchain improves the work process such that a more responsible adoption rate is achieved?

Yes, the process is very clear. I am already familiar with blockchain and the way you implemented is understandable. I like the usage of private keys, this would be a great first step towards a fully automated system.

2. Is the proposed blockchain method useful to the organisation?

Yes, I am sure this method will be helpful although challenging. Perhaps the checks, so the validation by all the nodes, might take too long leading to delays. Also, the system might need some scaling in terms of levels of data.

3. Is the method generalizable, i.e. applicable in other contexts?

Definitely. With the consortium blockchain you mentioned, this method can be implemented in the process of parties such as Rijkswaterstaat and the Dutch Police Department. Note that some standardisation is required though and of course different conditions. Perhaps by clustering and filtering the data blocks, the usage might be eased as well. Furthermore, as you mentioned, future revenue models and collaboration possibilities are of course highly appreciated for our on-going projects. Think about subsidy projects of farmers whereby blockchain allows a trustworthy transaction based on 100% reliable data. This can hence in a different context be very helpful.

4. What are the strengths, weaknesses and potential improvements of the design?

Strengths are of course as said in the presentation, related to the transparency and enhanced security of the system. These are important factors which will benefit us. In terms of weaknesses or improvement points, the validating part as said before might take too long. Perhaps if you cluster data (e.g. all imagery data of forests) the blocks are simplified such that not every picture must be validated on an individual basis. Also, you could scale the data by giving certain scores or weight (low or high level) for the sensitivity of the data. In this way, data access might be scaled as well. Last point is regarding the implementation of the system. How fast can we implement this is an important factor to be considered. Perhaps we can take small steps towards blockchain by setting up the conditions already.

E2: Head of Department Trade & Digital Surveillance (NVWA)

1. Is it clear how blockchain improves the work process such that a more responsible adoption rate is achieved?

Yes, it is very clear and simultaneously very challenging. The process is presented very clear although the implementation is not so simple. In fact, I liked your presentation and use-cases that much that I would like to use it for a presentation next week. If get your approval, I will mention your name and hopefully this will help us for the construction of a so-called 'Information House'.

2. Is the proposed blockchain method useful to the organisation?

Yes, especially if you look at the potential revenue models and collaborations in the future. A revenue model would for instance be in the novel essence of inspection methods. Furthermore, the case of sharing data with other governmental agencies will be made more secure. More specifically, us-

ing blockchain will compete the current obstacles of security and access management. In summary, blockchain seems to be the solution for a number of issues that we currently want to solve.

3. Is the method generalizable, i.e. applicable in other contexts?

Yes, see the previous answer. Using Blockchain in a transparent and accountable manner with other governments (with some limitations) is highly favored. We have some on-going projects such as Drone2Go where this is a key point of interest. The NVWA is in a transition from mainly sensory perception to predominantly digital perception. A data-driven way of working is emerging and blockchain could have great added value here. Blockchain can be seen as a building block for the new digitized forms of inspection.

4. What are the strengths, weaknesses and potential improvements of the design?

Strengths are already mentioned and of course its transparency, applicability and the logical way it works. However in terms of weaknesses, the technique is too 'young' and hasn't proven itself yet. This might be an issue for the governmental bodies in The Hague and Brussels. They might have a hard time accepting the implementation of this technology for our current operations. Therefore small steps must be made towards blockchain which is definitely doable.