MSc Program
Engineering Management

Managing change and development in a complex socio-technical system: An Air Traffic Management Case Study

A Master's Thesis submitted for the degree of
"Master of Science"

supervised by
Prof. Larry Stapleton

Mag. Anna Weszelits, Bakk.

00403456

Vienna, 29.03.2020

Affidavit

I, **MAG. ANNA WESZELITS, BAKK.**, hereby declare

1. that I am the sole author of the present Master's Thesis, "MANAGING CHANGE AND DEVELOPMENT IN A COMPLEX SOCIO-TECHNICAL SYSTEM: AN AIR TRAFFIC MANAGEMENT CASE STUDY", 78 pages, bound, and that I have not used any source or tool other than those referenced or any other illicit aid or tool, and
2. that I have not prior to this date submitted the topic of this Master's Thesis or parts of it in any form for assessment as an examination paper, either in Austria or abroad.

Vienna, 29.03.2020

Signature

Acknowledgements

I want to express my gratitude to my academic supervisor, Professor Larry Stapleton, for his valuable and targeted guidance throughout the process of planning and writing this thesis.

I also want to thank my partner and family for their patience and support during the time I invested in the attendance and completion of the MSc Engineering Management Program whilst being employed full time.

Last but not least, I thank my colleagues for contributing to this work with their expertise.

Abstract

The study at hand examines change and development of Air Traffic Management systems in the context of Complex Systems Theory. A literature review of Systems Theory, Complexity Science and Engineering Management as well as an account of Air Traffic Management and the role of safety provide the groundwork for analysis and highlight the necessary considerations when dealing with complex socio-technical systems in general and Air Traffic Management Systems in particular. Building on the concepts discussed in the literature review, the study explores which internal and external complexity drivers impact system development at an Organization providing Air Navigation Services and suggests that safety culture and safety regulation have not yet reached the end of the line in terms of acknowledging the role of complexity in the change management process.

Key words: Complex Systems, Systems Engineering, Requirements Engineering, Holism, System Development, Air Traffic Management, Air Navigation Services

Table of Contents

1 INTRODUCTION 1

1.1 Relevance and contribution 1

1.2 Research objectives...3

1.3 Research Questions...3

1.4 Thesis structure...4

2 SYSTEMS AND COMPLEXITY: THEORETICAL BACKGROUND AND LITERATURE REVIEW 5

2.1 Introduction...5

2.2 Fundamental system terminology and attributes 5

2.3 System Thinking: Concepts and methods..8

2.3.1 Synergy...8

2.3.2 Emergence and emerging system properties 9

2.3.3 Holism 9

2.3.4 System dynamics..12

2.4 Exploring Complexity..12

2.4.1 Complexity versus complication...13

2.4.2 Technology as a source of complexity..13

2.4.3 Complexity and Unpredictability 15

2.4.4 Consequences of increased complexity 17

2.4.5 Complexity Drivers 17

2.5 Systems Engineering 19

2.5.1 System Architecture...21

2.5.2 Requirements Engineering and Management 22

2.6 Selected System Theories and Concepts..26

2.6.1 Socio-Technical Systems (STS)..26

2.6.2 (Joint) Cognitive Systems (JCS) 27

2.6.3 Complex Products and Systems (CoPS) 28

2.6.4 Large Technical Systems (LTS)..29

2.6.5 Innovation as a product of systems...30

2.6.6 Complex Network Theory 30

2.7 Chapter Summary..33

3 AIR TRAFFIC MANAGEMENT AND SAFETY: THEORETICAL BACKGROUND AND LITERATURE REVIEW 34

3.1 INTRODUCTION 34
3.2 THE FORMATION AND ORGANIZATION OF AIR TRAFFIC MANAGEMENT (ATM) IN EUROPE 34
3.3 TERMINOLOGY IN THE ATM DOMAIN 35
3.4 AIR NAVIGATION SERVICES AS A SYSTEM OF SYSTEMS 37
3.5 UNCERTAINTY IN ATM 39
3.6 SAFETY IN AIR TRAFFIC MANAGEMENT 40
3.6.1 SAFETY CULTURE 42
3.6.2 A NEW APPROACH TO SAFETY IN ATM 45
3.7 CHAPTER SUMMARY 49

4 RESEARCH PROCESS 50

4.1 INTRODUCTION 50
4.2 METHODOLOGY 50
4.3 DATA COMPILATION 52
4.4 BENEFITS AND LIMITATIONS OF THE RESEARCH APPROACH 53
4.5 CHAPTER SUMMARY 53

5 RESULTS 54

5.1 INTRODUCTION 54
5.2 BACKGROUND AND CONTEXT 54
5.3 CODING RESULTS 54
5.3.1 THE UNKNOWN UNKNOWNS 55
5.3.2 DYNAMICS OF THE ENVIRONMENT 55
5.3.3 "QUICK AND DIRTY" SOLUTIONS THAT BECOME PERMANENT 56
5.3.4 EMERGENCE 56
5.3.5 SYSTEM LIMITS 57
5.3.6 VENDOR LOCK-IN AND PARTNERSHIP ISSUES 57
5.3.7 MATURITY 58
5.3.8 THE THIN LINE BETWEEN SAFETY AND CAPACITY 58
5.3.9 AIRBORNE EQUIPAGE 58
5.3.10 COST-BENEFIT-ANALYSIS ISSUES 58
5.3.11 DYNAMIC NEEDS AND FUZZY REQUIREMENTS 58
5.3.12 PERPETUATION OF OPERATIONS BEATS IMPROVEMENT 59

5.3.13 SAFETY IN THE CONTEXT OF SYSTEM CHANGES..59
5.4 CHAPTER SUMMARY..60

6 DISCUSSION OF FINDINGS AND OUTLOOK..61

6.1 INTRODUCTION..61
6.2 RESEARCH FINDINGS..61
6.3 OUTLOOK..65

REFERENCES..66

LIST OF FIGURES...69

LIST OF TABLES..70

LIST OF ABBREVIATIONS...71

1 Introduction

While working on the literature review for this study, I came across the following quote, and it struck me as the ideal entry point for explaining my aim with this work:

> *"Look at the news as organizations struggle to meet new demands on their performance, how to be more efficient under resource pressures, or how to recognize and exploit opportunities created as the technology baseline advances. Back and forth the comments cycle: Are people the solution or are people the problem to be solved? Is human performance the key to achieving goals or is human performance the limit to be overcome? People: sinners or saints? An old debate to be sure, but a false position that continues to fail to improve performance or safety as it assumes the wrong unit of analysis and design. The path to success begins with recognizing the paradox that, simultaneously, we are both the source of success and of failure as we create, operate, and modify human systems for human purposes."* (Woods and Hollnagel 2006: 1)

In my current professional activity in Air Navigation Services, I frequently observe and experience this organizational struggle. The quest for increased efficiency and capacity (i.e. the ideal of fewer Air Traffic Controllers handling more flights) while still maintaining high levels of safety and remaining cost efficient is a tricky task for organizations. In socio-technical systems such as Air Traffic Management or Aviation in general is one, these goals often translate into new requirements for technical systems and implementation of these requirements is becoming increasingly difficult as the level of system complexity rises. But why exactly is that? What are these complexity drivers exactly and why do they become so virulent in system development? What role does safety play in all this? These are the questions that lead to this work.

1.1 Relevance and contribution

In the context of Complexity Theory applied to Air Navigation Services (ANS) or Air Traffic Management (ATM) a great deal of the research falls in the category of analyzing human-machine-interaction at the air traffic controller working position: The visible front end of the Air Traffic Management System.

James Reason's much-acclaimed Swiss Cheese Model reveals, by means of describing accident trajectories that penetrate weak points of multiple safety layers – for which the mid-air collision of Überlingen in 2002 is a tragic, real-life example – that Air Traffic Management is a multi-layered, inherently complex high risk system. Consequently, the aforementioned controller working position constitutes only the tangible tip of the iceberg of Air Traffic Management as a complex system of systems that unfolds underneath the surface: The back end, so to speak.

Reason notes that the complexity of such systems tends to make them opaque to operators and impossible for individuals to understand in their entirety (Reason, 1998). This becomes especially relevant in a reality, where digitalization continues to create even higher degrees of complexity: Previously discrete services (e.g. radio communication, radar), become increasingly interwoven/interdependent in their further digital processing.

Whereas Reason's focus lies on engineering a safety culture around the operation of such systems throughout their lifecycle, I would like to deal with the role complexity plays in the process of continued system development, during which new requirements are introduced, analyzed and may trigger changes to the system.

In order for systems development to avoid steering from opaqueness into utter darkness, already present complexity factors and applied safety measures need to be understood. The research aim of this work is to identify relevant complexity factors in a case study of a European Air Navigation Service Provider, with a focus on Air Traffic Management system development and change, with the intention of delivering a comprehensive picture of internal and external complexity influences on Air Traffic Management system architecture.

From an academic perspective, this study aims at delivering an inside account and analysis of a complex, high-risk socio-technical system such as Air Traffic Management is one.

From a practitioner's perspective, the solution-oriented application of Complexity Theory with the aim to solve real world problems is the core contribution of this work.

1.2 Research objectives

The research objectives of this work are guided by the following considerations and interests:

- Systems Thinking and Complexity Theory: Review and application potential to the research topic.
- Identification of the factors that continue to drive complexity into the socio-technical system architecture of a European Air Navigation Service Provider.
- Understanding in what ways Requirements Engineering acknowledges and takes into account these factors or not and resolves conflict between them.
- Analysis of the perceived clash between safety culture and digital innovation.
- Discussion of emergent behavior and uncertainty in Air Traffic Management System Development.

1.3 Research Questions

RQ1: What are the main internal and external drivers of complexity into Air Traffic Management System Architecture and what are their (potentially reciprocal) effects?

RQ2: In what ways has Safety Culture (relevant regulation as well as internal measures) responded to increased organizational and system complexity and how is this factored (or not) into the requirements engineering process?

1.4 Thesis structure

Chapters 2 and 3 contain the *theoretical foundations*. Chapter 4 and 5 provide an account of the *research process* as well as the *results*, and chapter 6 concludes with a *discussion* of the research findings:

Chapter 2	discusses various relevant concepts and theories on systems thinking, systems engineering, requirements engineering and complexity.
Chapter 3	outlines how *Air Traffic Management in Europe* developed, what it is composed of and impacted by and focuses on the relevance of safety and safety culture in *Air Navigation Service Provision*.
Chapter 4	gives an account of the *methodological approach* chosen as well as of the data collection through meeting participation.
Chapter 5	reports the results of the study.
Chapter 6	discusses the results of the study in the light of the research questions and concludes with an outlook and suggestions for further research.

2 Systems and Complexity: Theoretical background and Literature Review

2.1 Introduction

"A perfectly optimized system is a set of suboptimal subsystems. If teams try to optimise each subsystem there will be conflict." (Hood et al. 2008: 2)

This chapter sets out to review and discuss the fundamentals of Systems and Complexity Theory as well as Systems and Requirements Engineering. The concepts presented in this chapter set the scene for the subsequent chapter on Air Traffic Management (ATM) and Safety.

2.2 Fundamental system terminology and attributes

In this section, let us have look at some fundamental system terminology, as described by Haberfellner et al. (2015: 31ff):

System, elements and relations: Many phenomena in everyday language are described as "systems", such as the solar system, the economic system, the education system. All these examples are united by the connectivity they entail. A system is defined as a system, because it is made of elements that stand in relations to one another and form a perceived whole. These relations can be material flow relations, information flow relations, position relations or cause and effect relations. Elements themselves can be seen as their own system. (ibid.)

System boundaries and environment: A system boundary is a more or less arbitrary demarcation between the system and its environment. The systems discussed here are open systems, meaning they not only exhibit relations between elements within the system, but also with the system environment. The periphery or environment of a system is made up of elements or systems outside the boundaries of the system in focus and are sometimes described as **peripheral systems**. What separates a system from peripheral system and justifies boundary setting is the degree of relations. The predominance of the internal bond is what separates a system from its environment, and depending on the perspective, this boundary may be variably set. (ibid.)

Structure of a system: Elements and relations exhibit a certain order. This structure of a system follows patterns and principles, such as hierarchical, network, historical, star or feedback structures. (ibid.)

Subsystems: The term subsystem is useful when zooming into a system element to capture it as a system in itself. (ibid.)

Hyper- or super-system: An aggregation of multiple systems into one comprehensive system. (ibid.)

System of systems: This is a term – sometimes also abbreviated to SoS – gets used in more recent scientific literature. There is no clear differentiation from sub- or hyper-systems. System of systems describes a system that consists of multiple individual systems 1) which aren't exclusively dependent from its super-ordinate system, but which have a standalone use, accomplishable independently from other systems and 2) which each can be developed and procured independently. (ibid.)

System hierarchy: When a system is partitioned along levels or steps, a specific structure – a system hierarchy – is the result and reveals the relativity of the terms of system, subsystem and element. (ibid.)

Black, grey and white box: The term black box is used when the inner structure of a phenomenon is – temporarily – unimportant. What matters is solely the function (or use) as well as the existing or desired inputs and outputs (results). Black box observation is an important tool for reducing complexity. White box observations are used when exact relations between output and input are of interest, or when the detailed observation of – analytically derived – inner relations is desired. A grey box is a system observation, in which a system is either only roughly structured or parts of the system are structured in more, others in less detail. (ibid.)

System aspects/types: Each system can be described from multiple viewpoints. Depending on the point of view or filter that is chosen, certain system properties of the system, its elements and relations come to the fore. Each description of this kind serves as one system aspect (of many). (ibid.)

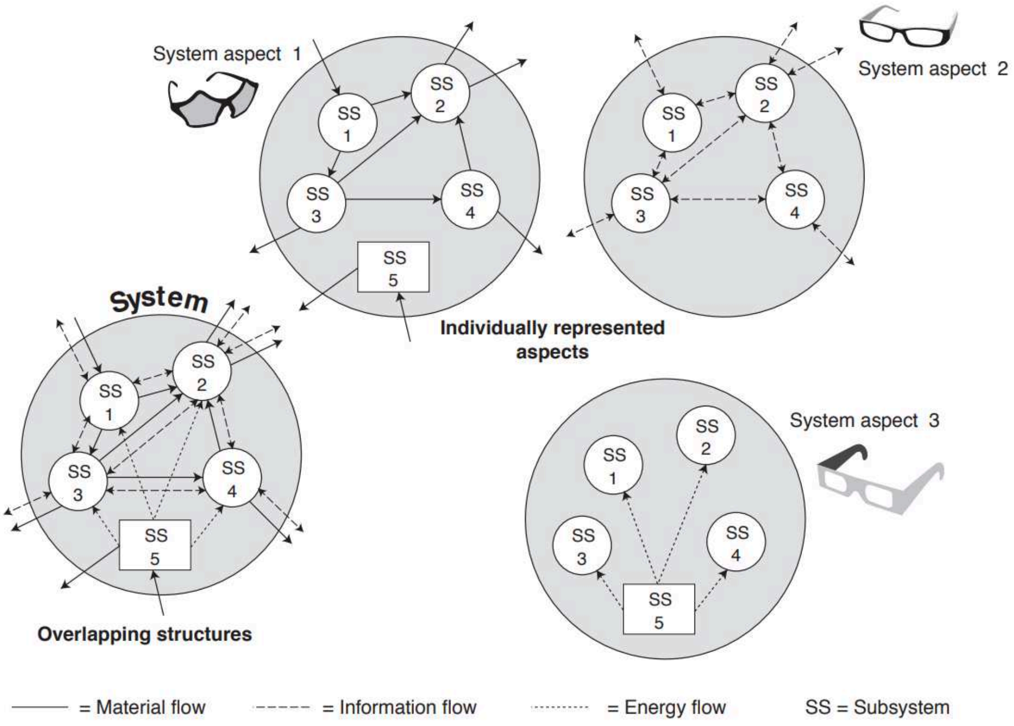

Figure 1: Aspects of a system (Haberfellner 2019: 10)

Simple system: A simple system is made up of few elements which are firmly and permanently connected and exhibit a low intensity of relation. The simple system serves as a basic model. An increase in number and diversity of components and relations as well as of more dynamic interdependencies and cross-links between elements results in three further system types: Strongly cross-linked, complicated systems, dynamic, complicated systems and complex systems. (ibid.)

Strongly cross-linked, complicated system: Such a system is characterized by its high number of elements and their diversity. Elements are connected statically. Due to the size of the system, an explicit description of the system and its behavior is oftentimes not possible. (ibid.)

Dynamic, complicated system: Such a system exhibits temporal, often non-linear convertibility of the connection between elements as to their interaction type, strength and structure, but with a low degree of interdependencies (in number and strength). However, due to their dynamic nature, it is difficulty to describe them in a quantitative manner as well as to predict system behavior. (ibid.)

Complex system: A system that is characterized by a high number of diverse elements and dynamic connections is complex. Usually, in complex systems , system-wide interdependencies are the case. These are the systems, systems engineering methods focus on. (ibid.)

2.3 System Thinking: Concepts and methods

Crawley et al. define system thinking as the act of thinking about a problem or as system. System thinking can be used as a means of

- understanding the behavior and/or performance of a current system
- assessing consequences of a potential system change
- informing decisions that concern the system
- supporting the system architecture (i.e. the design and synthesis) of a system (Crawley et al. 2016: 22f)

with a system being defined a set of entities including their (either static or dynamic) relationships, whose functionality is greater than the sum of the individual entities. (Crawley et al. 2016: 23) System architecture in turn can be defined as *"an abstract description of the entities of a system and the relationship between those entities"* (Miller in Crawley et al. 2016: 23)

But what exactly makes systems greater than the sum of its parts? This is where the system effects of synergy and emergence come into play. Both these effects are essentially based on the non-linearity of system relations.

2.3.1 Synergy

Mallikarjan and Smith (2015) highlight synergy among functions as well as synergy among components. On component level, positive synergy usually stands for increased reliability (e.g. multiple rollers on a conveyor belt as a simple example), whereas negative synergy describes unexpected interactions among components. On function level, synergy describes the (positive or negative) effect of the existence of one function on another function. Here, Mallikarjan and Smith give the example of a military ship with the given functions "floating", "sailing", "shooting" and "resisting". In a case of positive synergy, the sailing function can be seen as an aid to the floating function.

2.3.2 Emergence and emerging system properties

Mallikarjan and Smith define emergence as something that *"occurs when properties that are not present at a lower level arise at a higher level. In other words, the whole at a higher level is fundamentally different that any predictable consequence of combination of elements or properties at a lower level"*. (2015: 10)

Crawley et al. (2016: 24) define emergence as *"what appears, materializes, or surfaces when a system operates"*. Emergence can be detected on the function as well as on the performance level of a system. Function describes what a system does and when a system is designed, it is designed in a way so the intended, primary function of a system is able to emerge. At the same time, other unintended functions (desirable or undesirable) can and will emerge. This is the essential aspect of systems. On top of the emergence of functions, performance (i.e. *"how well a system operates or executes its function(s)")* also emerges within systems.

Crawley et al. (2016: 25) highlight the following emerging *"ilities"* as attributes of operation within systems, who differ from emerging functions and performance mostly due do the fact that their value does not become apparent immediately, but rather over the lifecycle of a system:

- **Safety**
- Robustness
- Maintainability
- Operability
- Reliability

On top of those *"ilities"*, emergencies are suggested as a discrete class of severe, unintended and undesirable emergent behavior.

2.3.3 Holism

Form is the informational or physical embodiment of a system – a shape, configuration, arrangement or layout – that exists or may exist. Form remains static over a certain period of time and it is needed to deliver function. **Function**

describes the activities of a system, which cause or contribute to performance. (Crawley et al. 2016: 28f.)

A system can be considered as an entity with a certain form and certain function(s) and it can, in itself, be decomposed/broken down into further entities, each of which again are characterized by a certain form and certain function(s). The difficulty of decomposing a system entity into entities along internal boundaries depends on the interconnectedness and dependencies between those entities. Decomposition may be unambiguous with clearly distinct elements, slightly more challenging but still clear enough with modular entities and most difficult with integral entities, whereas information systems are usually characterized by a high level of integrality. (Crawley et al. 2016: 33)

Holistic thinking insists that things are intimately connected and that deliberately thinking about the whole is a necessity. Crawley et al. name the following holistic principles (2016: 34):

- All things exist and act as wholes and cannot solely be understood through the explanations of their parts.
- All aspects of a system as well as any potential influences and consequences of anything that might interact with it need to be taken into account.
- Anything of potential importance to a specific question or problem needs to be considered (entities and their relationships, the system context etc.).
- Holistic thinking methods include structured and unstructured brainstorming, frameworks, multiple perspective thinking, context thinking.
- The goal is to identify as many unknown-unknowns as possible and transfer them into known-unknowns.

Holistic thinking generates a lot of information, of which the system thinker then needs to separate critical and consequential information from non-critical and non-consequential information: The principle of focus. Further, abstraction is used to focus on important details of an entity (and environment) and hiding any details or complexities that are not necessary to consider. The following abstraction principles are relevant (Crawley et al. 2016: 35f.):

- Abstractions of form and function shall allow for the representation of important information on the surface and conceal less relevant details.
- Abstractions shall allow for the representation of appropriate relationships.
- Abstractions shall consider the appropriate level of decomposition or aggregation.
- Abstractions shall be minimized to what is needed to effectively represent the aspects of the system.

As part of system thinking, it is also necessary to clearly define **system boundaries** and thereby separate systems from their context. This limitation is needed for two reasons: Either because we, as humans, are not capable of considering a more extensive set of entities or because we, out of our human judgment, simply do not consider it useful. (Crawley et al. 2016: 38)

Haberfellner et al. (2015: 39f.) also understand the illustration of systems and complex relations as a central principle of system thinking. The appraisal of problem relevance and expediency of the chosen abstraction are essential to system thinking. Here, three approaches to arrive at useful conclusions about a specific system are highlighted:

1. **Environment/periphery approach**: With this approach, the system in itself is disregarded at first, it is seen as a black box. Instead, focus lies on the relations between the system and its environment. Asking about the kind and extend of external factors provides a good entry point.
2. **Input/output approach**: The central question in this approach is which relevant impacts and inputs from the environment/periphery, in connection with the possible behavior of a system has which effects and outputs relevant to the environment. This approach supports a rough characterization of problem fields (and potential solutions) and provides a good basis for the more detailed structure-oriented approach.
3. **Structure-oriented approach:** This approach focuses on the elements of a system and their relations and specifically those mechanisms of action and processes which are of dynamic nature. This perspective supports the

analysis of how output is generated from inputs, or how input can be transformed into a specified output.

These approaches also reflect the order in which system thinking shall be applied. However, depending on the point of view taken, any approach chosen will result in a system description that highlights one aspect but neglects the other: A necessity when handling complexity in an orderly fashion. (Haberfellner 2015: 44)

2.3.4 System dynamics

Languages like English, German, French are linear languages, meaning they transform everything we chose to express into a point of view (e.g. "x causes y"). This linearity leads us to focusing on one way relations instead of circular or reciprocal relations. However, usually the most difficult problems are the ones resulting from a network of interconnected reciprocal relations. In this sense, system thinking can be understood as a language that allows for the visualization of such relations and interdependencies. This is also where the power of graphic system representations comes into play. (Haberfellner 2015: 49f.)

2.4 Exploring Complexity

Geels (2005: 37) describes complex systems theory as *"an interdisciplinary research perspective, with intellectual roots in mathematics, linguistics, economics and biology. Complex systems theory is not (yet) so much a theory as a perspective for theorising and modeling system dynamics."* (Geels 2005: 37)

Complexity is inherent in system architecture. It is driven into systems by asking systems to provide more function, performance, robustness and flexibility. System complexity itself therefore isn't a negative system attribute, it is rather, a logical consequence of these demands. (Crawley et al. 2015: 49). While a differentiation between essential complexity (i.e. the level of complexity required to address a demand) and superfluous complexity (i.e. anything beyond the required level of complexity) is possible in theory, reality rarely proves as straight forward. Reymondet (2016: 27) mentions system part redundancy as an inconclusive example: Depending on the perspective, this redundancy could be seen as either gratuitous or essential.

2.4.1 Complexity versus complication

"Complex" and "complicated" are often used interchangeably, which may lead to a merely "complicated" system being described as a "complex" one. However, these notions do differ in meaning and it is worth keeping them apart:

Garnsey and McGlade (2006: 4) differentiate as follows: A complicated system is one that can be understood and explained through disassembly and re-assembly of its components, meaning a system that can be explained through the description of its component parts, like a watch. Hence, complication can be understood as a quantitative escalation of what is theoretically reducible: A weakly complicated system comprising a simple hierarchical structure and a strongly complicated system comprising a hierarchical structure with circuits of influences. A complex system on the other hand is one, whose components interact in a non-linear manner and are also connected through various feedback loops. A complex system can therefore not be understood by merely isolating and describing individual components.

The view of Crawley et al. (2016: 50) is slightly different. While complexity is understood as a necessity, complicatedness is seen as something that should be avoided: *"Build systems of the necessary level of complexity that are not complicated!"*

2.4.2 Technology as a source of complexity

Woods and Hollnagel (2005: 1f.) describe three main driving forces which lead to the development of their "Cognitive Systems Engineering" (short: CSE) approach to deal with complex systems:

1. The increasing complexity of socio-technical systems, due to an unprecedented growth in the power of applied information technology and ultimately leading to computers becoming the dominant medium for work and interaction, while at the same time creating new fields of work.
2. The problems and failures created by clumsy usage of emerging technologies as often, practitioners did not have sufficient time to adapt to the growing complexity of their work environment. This development led to

real world failures of complex systems, which called attention to human factors and the buzzword "human error".

3. The realization, that humans could not be viewed as mere information processing systems and that existing linear models were inept to capture human-machine interaction in its entirety.

In reference to the Kuhnian concept of paradigm and paradigm shifts (Kuhn 1967) Woods and Hollnagel (2005) argue, that information processing represents a paradigm, whose positive innovatory aspects initially attract more attention than its negative aspects. While the quick application and integration of information technology into our everyday lives was driven by the initial enthusiasm, it took decades for the negative aspects of this paradigm to emerge as a stumbling block for further development.

Woods and Hollnagel (2006: 18) point out the "law of stretched systems", a concept originally coined by Lawrence Hirschhorn: *"Every system is stretched to operate at its capacity; as soon as there is some improvement, for example, in the form of new technology, it will be exploited to achieve a new intensity and tempo of activity."*

Whenever a new *black box* technology is introduced, the following consequences are observed by Woods in his studies:

- New capabilities create new increased demands
- New capabilities create new complexities
    - through increased coupling and dependencies across respective system components
    - as a result of a higher speed of operations
    - as a result of "clumsy" use of new technological possibilities
    - as an unintended side effect of design intent
- New complexities result in adaptations of practitioners
    - to exploit capabilities due to a pressure to meet operational goals
    - to work around complexities
- These adaptations then may lead to

- the occlusion of complexities from designers and after-the-fact-reviewers
- Failures occasionally breaking through these adaptations, when they are incomplete. (Woods 2006: 18f.)

2.4.3 Complexity and Unpredictability

Inevitably, increased system complexity also leads to increased task complexity (Perrow: 1984). Furthermore, chaos, shall be acknowledged as an intrinsic property of complex systems, undermining the idea that future system behavior is scientifically predictable. In fact, a complex, chaotic system provides increased degrees of freedom, which enable new, unpredictable pathways (Garnsey and McGlade 2006: 5f.). Unpredictable pathways may and will in turn also include the occurrence of problems and major malfunctions. Referring to the Challenger and Columbia space shuttle accidents as well as general issues with delays in every launch, Seife (1999: 2) describes the space shuttle as a system, whose complexity renders it nearly unmanageable.

When introducing new technologies, Woods and Hollnagel (2005: 4) point out how expectation and reality are rarely a match: *"Some of the explicit motivations for putting technology to use are reduced production costs, improved product quality, greater flexibility of services, and faster production and maintenance. It need hardly be pointed out that these benefits are far from certain and that a benefit in one area often is matched by new and unexpected problems in another. Furthermore, once the technology potential is put to use this generally leads to increased system complexity. Although this rarely is the intended outcome, it is a seemingly inescapable side effect of improved efficiency or versatility."*

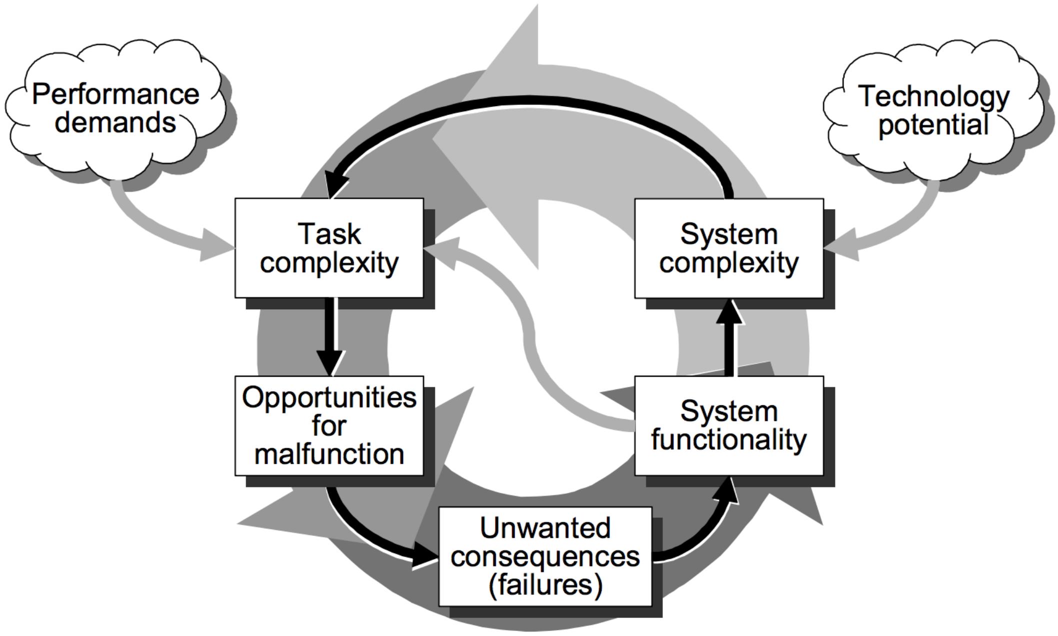

Figure 2: The self-reinforcing complexity cycle (Woods and Hollnagel 2005: 4)

Woods and Hollnagel acknowledge, that the "self-reinforcing complexity cycle" only provides a simplified view which makes the consequences of system complexity look worse than they actually are, because it does not depict the very real ability of systems to self-correct. This is done with the intention to point out the following:

- Systems and issues should rather be considered as coupled than as independent.
- The context of events and relation is important. Human activities shall never only be understood as reactions to events, but rather in an embedded manner.
- System control is integral, as unexpected system behaviour and situations will occur and need to be detected when they do. (Woods and Hollnagel 2005: 6)

Unexpected system behavior can also be described using the concept of uncertainty. Here, one needs to distinguish between objective and subjective uncertainty. Objective – or fundamental – uncertainty means a system does not evolve in a deterministic way and it is therefore inherently impossible to exactly know its state.

Subjective uncertainty, also sometimes referred to as hidden determinism, describes a system or artifact, that itself is deterministic, but whose state can nevertheless not be exactly known due to external dynamics which impact inputs to the system (this holds true for systems, in which human factors play a significant role. (Rivas and Vazquez in Cook and Rivas: 2016: 42)

2.4.4 Consequences of increased complexity

In its strive for higher efficiency, increased system complexity will challenge its limits of safe performance. While the number of incidents and accidents remains constant, the consequences will be more severe, as the failure of one system is likely to have an effect on other systems. This results in new system demands for design, implementation, management and maintenance. Another issue that comes with increased integration of information technology systems is the amount of data these systems produce: *"The belief that more data or information automatically leads to better decisions is probably one of the most unfortunate mistakes of the information society."* (Woods and Hollnagel, 2005: 7)

Sheard (2010) identifies the following contributors to and effects of complexity:

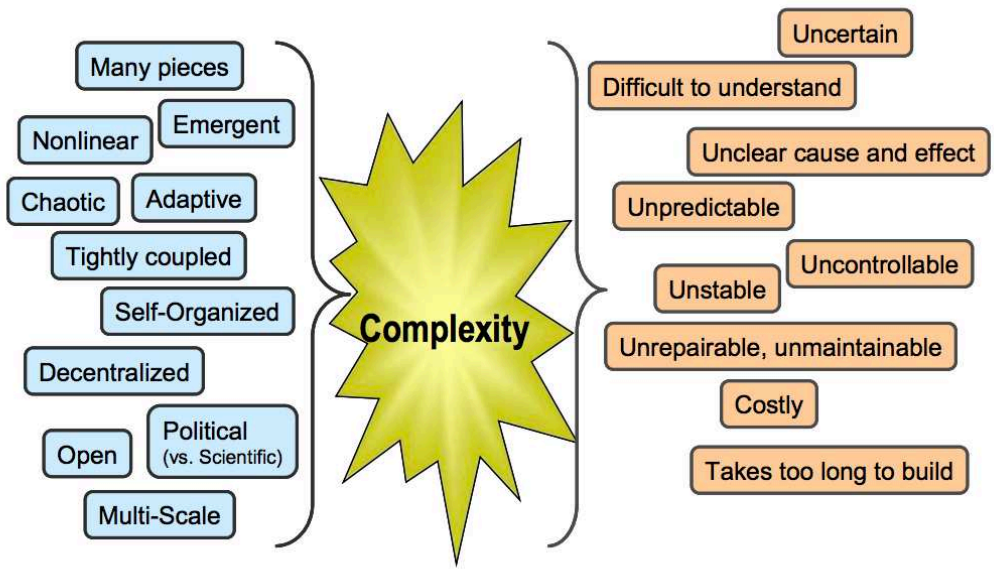

Figure 3: Contributors to and effects of complexity (Sheard 2010: 936)

2.4.5 Complexity Drivers

While considerable literature exists on the topic of complexity drivers in the area of logistics (Piya et al. 2017; Kohr et al. 2017; Seradarsan 2013; Meyer 2007) as well as overall manufacturing (Shafiee et al 2019; Vogel and Lasch 2016) this does not hold true for the analysis and differentiation of complexity drivers in overall Complex Systems Theory.

A driver, according to Business Dictionary[1] is defined as a condition or Rcausing *subsequent* conditions or decisions to occur as a consequence of its own occurrence as well as an element of a system with a major or critical effect on the associated elements or the system as a whole. Krizanits (2015) highlights, how complexity drivers can cause for turbulence and new functional models to occur within a system.

According to Vogel and Lasch (2016: 2) the identification, analysis and understanding of complexity drivers poses the first step in the development of a strategy to handle complexity. As one of the leading research questions of this work is the examination of complexity drivers in Air Traffic Management, the work done in the field of logistics and manufacturing can be consulted for potentially wider applicability, by analogy.

Seradarsan (2013) differentiates between static, dynamic and decision making complexity drivers in logistics. Further, she categorizes these drivers according to their origin into internal, supply/demand interface as well as external/environmental drivers. Shafiee et al. (2019) separate between static and dynamic components of complexity as well as internal and external factors. Here, the static complexity factor represents the basic product and management complexity, whereas the dynamic complexity factor is the amount of change (additional to or less than basic complexity) for a given product. The study results of Shafiee et al. show a higher complexity impact of external drivers than internal drivers, but note that while the impact of external drivers is higher, they cannot be controlled by the respective organization and therefore their research puts a stronger focus on the management of internal drivers.

[1] http://www.businessdictionary.com/definition/driver.html

Kohr et al. distinguish exclusively between internal and external drivers and highlight the need for understanding how these drivers impact products and processes and identify the following external and internal drivers (Kohr et al. 2017: 55):

External complexity drivers	**Internal complexity drivers**
• uncertainty of delivery (quality) • uncertainty of delivery (time) • number of suppliers • dynamic of competition • volatility of customer demand • variety of customer requirements • number of customers • political factors • legal factors	• Corporate Culture • Organizational structure • number of distribution levels • dynamic of production technology • value added step • degree of cross-linking • dynamic of product technology • product structure • dynamic of product portfolio • variety of products

Table 1: External and internal complexity drivers in Manufacturing (as identified by Kohr et al. 2017: 55)

The differentiation between internal and external drivers, as well as the consideration of decision making complexity will be of value for the case study for the case study embedded in this work.

2.5 Systems Engineering

In Systems Engineering (SE), system thinking is applied to the problem field as well as the solution. "Problem field" describes the system, in which problems are suspected. (Haberfellner 2015: 132)

According to their SE Handbook, NASA defines Systems Engineering as a *"methodical, multi-disciplinary approach for the design, realization, technical management, operations and retirement of a system."* (NASA 2007: 3f)

It is the objective of Systems Engineering to ensure a system is designed, built and operable so it fulfills its purpose safely and with a cost-effective balance of performance, cost, schedule and risk factors. All elements required for the production of system-level results need to be considered: hard- and software, equipment, facilities, personnel, processes and procedures. It is essential for Systems Engineering to put focus on the human element. System level results include the performance of the system, its characteristics, functions, behavior, qualities and properties: "*It is a way of achieving stakeholder functional, physical, and operational performance requirements in the intended use environment over the planned life of the system within cost, schedule, and other constraints. It is a methodology that supports the containment of the life cycle cost of a system. In other words, systems engineering is a logical way of thinking.*" (ibid.)

Systems engineering shall be understood as a holistic, transversal discipline, which aims at producing a coherent whole that is not dominated by a single discipline's perspective. It acknowledges opposing interests and potentially conflicting constraints and seeks to address them with a balanced system design. (ibid.)

In this conflict, the systems engineer may arrive at what NASA describes as the *"System engineer's Dilemma*":

- *"To reduce cost at constant risk, performance must be reduced.*
- *To reduce risk at constant cost, performance must be reduced.*
- *To reduce cost at constant performance, higher risks must be accepted.*
- *To reduce risk at constant performance, higher costs must be accepted.*

In this context, time in the schedule is often a critical resource, so that schedule behaves like a kind of cost. " (NASA 2007: 12)

The following figure shows how system design costs tends to get locked in at the early stages of design and development and how the cost for fixing problems is considerably higher at later life cycle stages, which underlines the importance of a holistic system design:

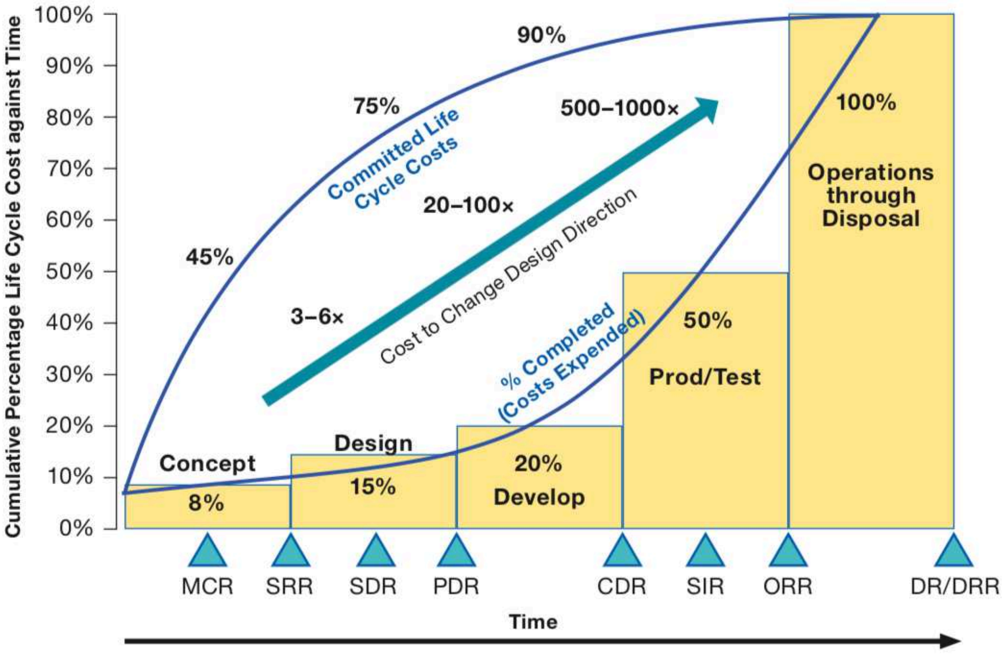

Figure 4: Life-Cycle Cost Impacts from Early Phase Decision-Making (NASA 2007: 13)

2.5.1 System Architecture

System architecture is the process of allocating functions to elements of a structure. While function means, what the system does an what kind of value it produces, form can be understood as the concrete medium of the function. The system elements and their structure create form. The following characteristics can be considered elements of a good system architecture:

- allows for competitive products
- fulfills the strategic goals of an organization
- ensures compliance with current and future rules and regulations
- is scalable and adaptable with little effort
- is “elegant”

It is the system architect’s role to translate functions into form as well as to define interfaces between elements. (Haberfellner et al. 2015: 183ff.)

2.5.2 Requirements Engineering and Management

Customers or users are usually able to describe their preferences/needs in a qualitative way, before translating them into a need statement, requirements or functional requirements. The criteria derived from these requirements are used to assess the fitness of systems, which often are not designed or integrated by the customer/user. (Mallikarjan and Smith 2015: 1)

Dick et al. (2017) put it like this: *"Before any system can be developed it is essential to establish the need for the system. If the purpose of a system is not known, it is unclear what sort of system will be developed, and it is impossible to determine whether the system, when developed, will satisfy the needs of its users. Forest Gump summed it up quite nicely when he said: If you don't know where you are going, you are unlikely to end up there."*

While requirements engineering is vital element of SE, it has developed into its own field of research as well: *"Requirements engineering (RE) is the branch of systems engineering concerned with the desired properties and constraints of software-intensive systems, the goals to be achieved in the software's environment, and assumptions about the environment."* (Ebert and Wieringa 2005: 453)

The below figure shows, why time invested into RE is time well spent: Requirement errors tend to result in a high effort of problem fixing during the further systems engineering process:

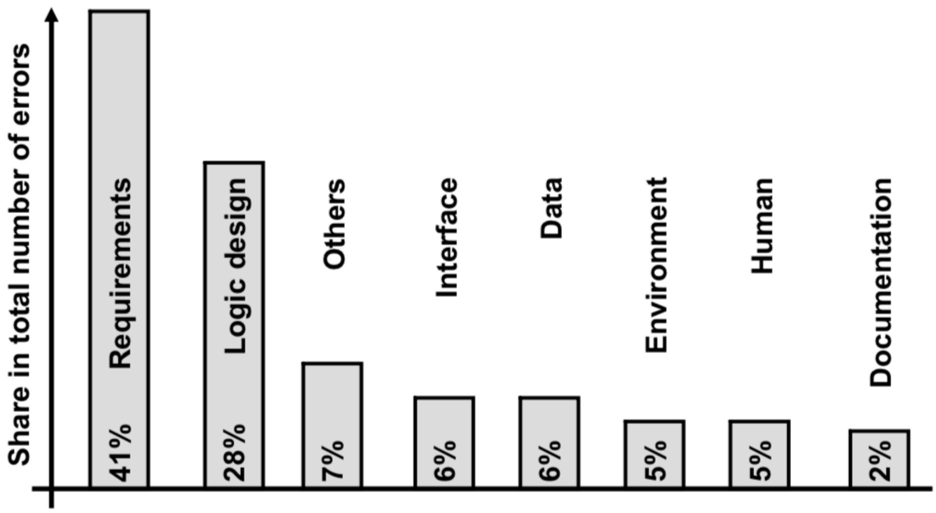

Figure 5: Share of errors in requirements in total number of errors (Hood et al. 2008: 13)

The three main goals of the RE process, according to Pohl (1994) are 1) to develop a complete system specification from a vague idea 2) to change informal system knowledge into formal representations and 3) to arrive at an agreed specification from a number of individual and potentially contradicting views. As this process requires decisions and in a human centered RE approach, this is also where the connection of RE and decision making comes into play. (Alenljung 2008: 12f.)

While there is no agreed definition on the notion of requirement, the IEEE 610 standard defines a requirement as, according to Machado et al. (Machado 2005:47) in Alenljung (2008: 13):

1. *"A condition or capability needed by a user to solve a problem or achieve an objective;*
2. *A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents;*
3. *A documented representation of a condition or capability as in (1) or (2)."*

Requirements are commonly divided into functional and non-functional requirements. While functional requirements describe what the system will do, non-functional requirements describe the quality of the system, driven by organizational, product or external needs. (Alenljung 2008: 14)

Suthcliffe (2002) separates both functional and non-functional requirements into goals, attributes and constraints (of for instance physical, legal, cost or environmental nature. Aurum and Wohlin (2005) see requirements fall into goal, domain, product or design level. (Alenljung 2008: 14)

However, independent from the classification chosen, requirements must be defined in a clear and unambiguous manner and to arrive at this quality, several iterations of requirements elicitation, analysis, negotiation, validation, documentation and management are usually required, as can be seen in the following figure:

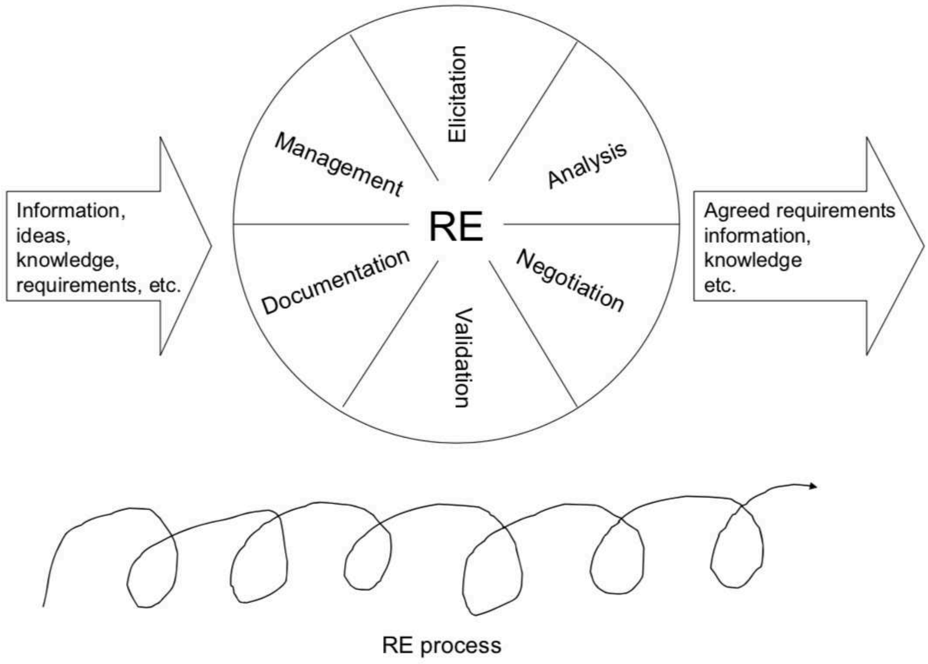

Figure 6: Requirements Engineering Process (Alenljung 2008: 17)

Requirements Management is a part of the RE process that is highlighted by Hood et al. (2008: 59) as *"all activities that are necessary to bring or keep the value of the requirements on a high level after the requirements have first been elicited and documented."* This also includes changes made to requirements as they must be managed and their impact on the relevant project must be understood. If requirements are not managed well, they will end up having little meaning, as their quality and applicability deteriorates when not kept up to date.

Dick et al. (2017: 36) highlight the necessity for acknowledging requirements at all of the following levels:

- Needs statement
- Stakeholder Requirements
- System component requirements
- Sub-systems component requirements

Consequently, concurrent work on requirements takes place at these different levels.

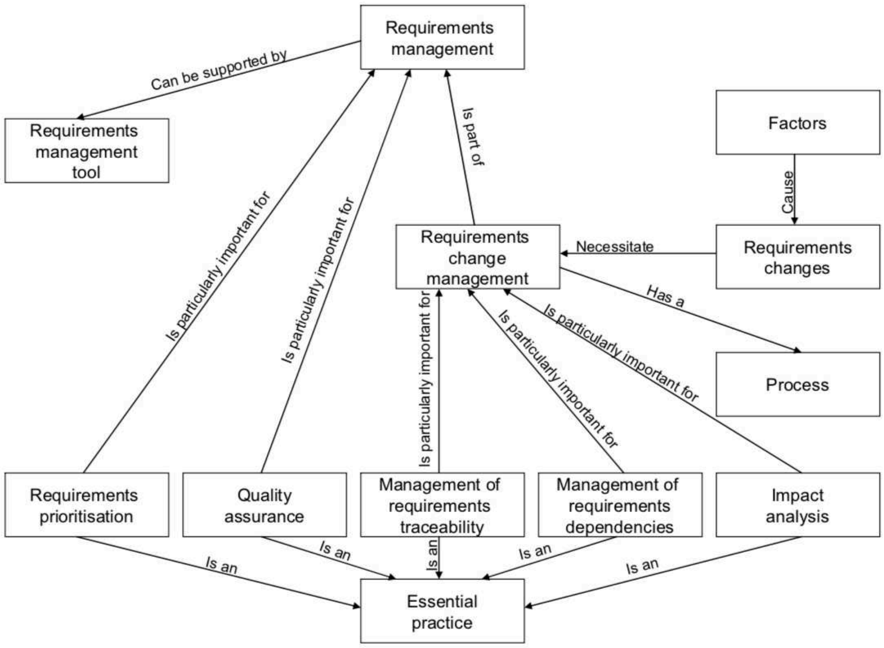

Figure 7: Requirements Management (Alenljung 2008: 29)

As mentioned earlier on, requirements engineering and decision-making are strongly connected in the management of system changes and according to Aurum and Wohlin (2003) as well as Evans et al. (1997) the Requirements Engineering Process can be understood as a decision process, requirements as decisions and requirements engineers as decision makers. (Alenljung 2008: 36)

The application of the eight factors of decision making as described by Orasanu and Conolly (1993) to Requirements Engineering leads us to the following view, as outlined by Alenljung (2008: 37):

1. **Ill-structured problems** that are taken up by a decision-making process rarely come out as clear and unambiguous requirements. The current state of practice reveals that decision problems are usually neither well described and understood, nor is the impact of these decisions comprehended enough
2. **Uncertain, dynamic environments** usually produce poor data quality and induce volatility into the decision-making process, due to fuzzy, inconsistent or incorrect information. The larger the system gets or the higher the number of system parts, the more design options there are and the larger and complex the decision space gets.

3. **Shifting, ill-defined or competing goals or values** cause conflicts and require trade-offs. Shifting goals include usability, security, reliability, maintainability, efficiency, portability and time-to-market.
4. **Action and feedback loops** are put in place so that the problem solving and decision-making may occur in an iterative manner. A loop problem is spoken of, when e.g. a main constraint is discovered too late in the process.
5. **Time stress** causes stress on the decision-maker and promotes ad hoc decision making.
6. **High stakes** are involved when the cost of the systems is significant or when the outcome is of significance.
7. **Multiple players** can actively be involved in the decision process, which adds complexity due to different expectations, perspectives, interests or constraints. However, what is often overlooked in the current state of practice is that by not taking into account all relevant stakeholder perspectives when making decisions, this can and usually will lead to problems at later stages of system development.
8. **Organizational goals and norms** are relevant and decision-making is bound to organizational context (norms, structures, procedures).

2.6 Selected System Theories and Concepts

The aim of this section is to present and discuss system concepts of value for the research problem.

2.6.1 Socio-Technical Systems (STS)

The term "sociotechnical system" was coined by Emery and Trist (1960) with the aim to challenge the technological determinism dominant at that time. This determinism postulated:

- the autonomy of technology
- the need for humans and human work to follow technical structures
- the expectation for humans to adapt to machines through training, which makes them replaceable if needed

In the late 1990s, the term was adopted in software engineering, as projects became more aware, that their objectives would alter not only the technical but also the social. (Maté and Silva 2005: viii)

STS is about providing an arsenal of descriptive methods as much as a research program for the optimization of the interaction between humans and technology. Central to STS theory is the assumption of equifinality of the socio-technical system, meaning that system goals can be reached in various ways and with various means, i.e. through adapted technology, change of behavior of people or new leadership structures in organizations. In the field of engineering and information technology, STS is also known under the names of "Re-Engineering" and Socio-Technical Systems Design (STSD). Social and technical sub-systems are understood as inherently and complexly connected to one another through functions, operations and values which leads to reciprocal effects. With technical changes, social effects need to be considered. (Karafyllis in Liggieri and Müller: 2019: 300f.)

2.6.2 (Joint) Cognitive Systems (JCS)

The Joint Cognitive Systems (JCS) approach does not define systems by what they are, but what they do. (Woods and Hollnagel 2005: 22)

JCS has developed as a concept in the realm of Cognitive Systems Engineering (CSE), which itself can be understood as a specific approach to Systems Engineering (for a discussion of Systems Engineering, see respective section above). In Cognitive Systems Engineering, the question is shifted from "how can limits be overcome" to "how can adaptability and control be supported"?: *"To study and design work, the unit of analysis is the joint cognitive system—not people and computers as separate components which then interact. Observing JCSs at work reveals processes of coordination and miscoordination as multiple parties contribute to handling evolving situations and achieving goals. Automation surprises are not simply a type of coordination breakdown at the sharp end of practice. The stories of coordination breakdown reveal a deeper surprise about automation as developers' oversimplifications about how JCS work lead them to miss predictable effects of technology change that create new complexities* *(workload, attention bottlenecks), miss how people adapt to work around complexities, and miss the actual functions in coordinated activity that require support."* (Woods and Hollnagel 2006: 142)

While JCS can be understood as closely related to STS, there is a much stronger focus of how human-machine co-agency evolves and leads to (unforeseen, by system design) workarounds. This approach will become relevant in chapter 2, as we discuss safety concepts in Air Traffic Management and specifically the concepts of "work as done" versus "work as imagined".

JCS puts focus on systems with the following characteristics:

- non-trivial functioning, meaning that more than a simple action is required to achieve a result or get a response from the technical system
- the technical system functions unpredictably or ambiguously to a degree
- the technical system is inherently dynamic, meaning that the pace or evolution of events in not user-driven, meaning that time pressure is a factor (Woods and Hollnagel 2005: 23)

The aim of JCS is not to distinguish between "the human" and "the machine" but to treat it as a whole. The cooperation and congruence of the system components (be it human or technical) is considered more relevant, than their internal processes and mechanisms. (Woods and Hollnagel 2005: 42f.)

2.6.3 Complex Products and Systems (CoPS)

The units of analysis within the Complex Products and Systems (CoPS) approach are, literally: products and systems and especially those that are technology- and capital-intensive and highly customized, such as flight simulation system, chemical plants, air traffic control systems, submarines etc. They are often designed to serve a particular purpose, based on user requirements. (Geels 2005: 32ff.)

The high level of customization leads to a close involvement of the user in the innovation process. The complexity in CoPS stems from the high number of specialized components involved, the breath and depth of (new) knowledge and skills involved in the design and production. (ibid.)

Usually, CoPS are not made by one company, but a network of companies, due to their high complexity and capital intensity. The typical organizational and management structure for CoPS is the project. the complex system gets broken up into discrete sub-systems or modules within a system architecture and are understood to communicate through standardized interfaces. As long as these interface standards, data transmission protocols and component specifications are are met, sub-systems are modifiable and improvable without affecting the workings of the remaining sub-systems. However, this modular approach has it limits, as innovation and change tends to not be confined to the module itself, but often impacts the other sub-systems or even the entire system architecture. This phenomenon is called "cascade dynamics". (ibid.)

In this sense, it can be argued that CoPS focuses too strongly on the individual modules or sub-systems while masking their wider embeddedness. Geels therefore suggests to pay attention to the interaction between the CoPS and LTS approach as well as between the CoPS and the STS approach for analytical synergies. (ibid.)

2.6.4 Large Technical Systems (LTS)

Large technical systems (LTS) theory focuses on a technology that consists of interrelated technologies, often within infrastructure networks with a certain geographic extent, such as telephone networks, railroad systems and the internet, while also considering the role of people, companies, text, contracts and legislation. Hughes (1987) points out the following five phases that LTS traverse 1) invention 2) development 3) innovation 4) growth, competition and consolidation and 5) momentum. He argues that invention is a continuous process and the task for development is to create a working configuration in the technical, economic and political sense. Once components are made to work, the phase of innovation is reached. In the growth phase, economies of scale become increasingly important, while, after continued growth, systems acquire momentum. (Geels 2005: 29ff.)

It is apparent that LTS has a strong focus on innovation and in general the ramp-up phases of systems, while it does not really look at system decline/end of life, thereby leaving out a relevant part of a system life cycle.

2.6.5 Innovation as a product of systems

In this concept, the system is not considered the actual topic of analysis, but rather, innovation is. Two relevant approaches are the sectoral system of innovation (SSI) as well as the technological systems approach. SSI can be defined as *"a system (group) of firms active in developing and making a sector's products and in generating and utilizing a sector's technologies; such a system of firms is related in two different ways: through processes of interaction and cooperation in artefact-technology development and through processes of competition and selection in innovative and market activities."* (Breschi and Malerba 1997: 131)

The technological systems approach looks at systems as networks that consist of dynamic knowledge and competence and are rather defined in terms of the flow of said knowledge and competence than flows of goods and services. It is an approach relevant also for the analysis of the emergence of new systems. (Geels 2005: 35)

2.6.6 Complex Network Theory

As all complex systems have interconnected components, Complex Network Theory (CNT) plays a central role in complexity science: *"[...] complex systems invariably involve networks. Generic topological properties are present in different complex systems, suggesting that some general principles govern the creation, growth and evolution of such networks."* (Cook and Zanin in Cook and Rivas, 2016: 9)

CNT is rooted in graph theory, which defines graphs are mathematical structures that show relationships between elements. In CNT, these elements are called "nodes" (or "vertices) and the connections between them "edges" (or "links"). Entities can be considered as assets in a way that the provide an intrinsic value to the network, but negative/unwanted examples are possible as well (such as the propagation of delay through a transport network as a domino effect, caused by a single flight). Graphs are considered "directed" when the direction of flows from one node to another is of relevance, and "undirected", when this is not the case. In addition, graphs can be weighted (i.e. associated to real life values, such as the number of flights in a given time window in an airport network, where each relevant airport represents a node. The value and power of network theory lies in its ability to abstract the underlying system structure independent from the nature of the system itself. While real life networks are often co-dependent, an edge in one network could be disruptive to an edge in another network (Cook and Zanin in Cook and Rivas, 2016: 10ff)

Network	Node	Edge	Flow	Disruption	Flow cost
Generic	Collection	Transport	Asset	Loss of capacity	Energy
Transport					
Air – flight-centric	Airport	Flight	Aircraft	Mechanical failure	Monetary
Air – pax-centric	Airport	Flight(s)	Passengers	Missed connection	Monetary
Urban (road)	Junction	Road segment	Vehicles	Bridge collapse	Monetary
Rail	Station	Track segment	Trains	Signal failure	Monetary
Goods	Warehouse	Road segment	Goods	Traffic congestion	Monetary
Services/utilities					
Water	Plant, reservoir	Pipe	Water	Pipe breakage	Energy
Electricity	(Sub) Station	Cables	Electrons	Cable breakage	Energy
Telecoms	Hub, router	Wire/fibre	Data packets: electrons/photons	Cable breakage	Energy
Biology/ecology					
Mammalian brain	Distinct grey matter regions	White matter fibre bundles	Electrical impulses; Neurotransmitters	Breakage (e.g. disease)	Energy
Fungal ecology	Branch point, fusion, tip	Cord (e.g. packed with hyphae)	Aqueous nutrients	Breakage (e.g. grazing)	Energy
Animal ecology	Habitat patch	Landscape segment	Species dispersal	Road segment	Energy

Table 2: Examples of Network Properties across multiple domains (Cook and Zanin in Cook and Rivas, 2016: 11)

It should be noted that many of these networks share common functional themes, such as capacity (expressed through varying metrics) or rerouting (e.g. in water distribution or telecommunication).

Complex system networks are commonly described on three scales:

- Microscale: Focus lies on the properties of a single node or link.
- Mesoscale: Focus lies on patterns and core-periphery structures. The Mesoscale provides a level between the separate study of single system elements and the system as a whole.
- Macroscale: Focus lies on the overall structure of and movement of information within the system as a whole. (ibid.)

Scale	**Mammalian brain example**	**Air transport example**
Microscale	A single neuron	A single flight
Mesoscale	A community of neurons, cooperatively processing a single stimulus	The community of flights of a single airline
Macroscale	The brain	The air transport network

Table 3: Introducing network scales (based on Cook and Zanin in Cook and Rivas, 2016: 13)

Here's an illustration of some metrics used in CNT in the context of a corresponding network scale:

Metric	**Classification**	**Basis**	**Summary Description**
Centrality	Microscale	Node	A generic term for metrics that identify the most important nodes in a network.
Clustering Coefficient	Mesoscale	Triplets of nodes	The fraction of pairs of a node's neighbours that are directly connected – thus a count of the number of triangles in the network, e.g. in the airport context
Global efficiency	Macroscale	Network	The ease of information flow between pairs of nodes.

Table 4: Selected complexity metrics (extracted from Cook and Zanin in Cook and Rivas, 2016: 14)

The power and success of CNT lies in its capacity to describe network characteristics shared by many real life systems. Network theory is able to show, for example, how, due to a biased attachment mechanism in networks, highly connected nodes gain additional links much more rapidly than smaller nodes, thus becoming hubs. Or as Cook and Zanin put it in short: *"The rich get richer."* (Cook and Zanin in Cook and Rivas, 2016:16ff)

2.7 Chapter Summary

The concepts described in this chapter show that there is a large number of valid viewpoints, from which complex systems can be deconstruct and analyzed The central common thought of systems thinking is interconnectedness of things and the necessity of a holistic approach, that knows where to draw the line between a system and its environment, depending on the problem focus. The concepts of Systems Engineering and Requirements Engineering, as well as the breakdown of the meaning of complexity and complexity drivers provides particular guidance to the study.

3 Air Traffic Management and Safety: Theoretical background and literature review

3.1 Introduction

With the concept of systems thinking from the previous chapter in mind, the aim of chapter three is to provide an overview of the development and status quo of European Air Traffic Management as a system of systems as well as to give an understanding of the paramount role of safety and safety culture in this system of systems.

3.2 The Formation and Organization of Air Traffic Management (ATM) in Europe

In the first years of aviation, air traffic was sparse enough for the pilots alone to take responsibility for aircraft safety. During that time, the aircraft captains were in charge of keeping safe distances to other aircraft as well as to obstacles and terrain. But the ability to guarantee flight safety in this way was gradually lost with increased air traffic density. This is the reason why air traffic control (ATC) from started to develop as a service delivered to aircraft from the ground. In its initiation phase, the biggest progress was made during WWII, when sovereignty of airspace started to develop as a concept. Governments were pushed into taking action to ensure and improve safety and efficiency of air traffic and in this environment, the International Civil Aviation Organization (ICAO) was founded in 1944 with the signing of the convention of International Civil Aviation and equipped with the mandate to establish procedures and declare standards for national governments to comply with. (Baumgartner in Cook, 2016: 1)

In EU member states the situation shifted from European States mostly financing air navigation services (ANS) themselves with a dedicated department for civil aviation to the setting up of corporate entities, who finance themselves through charges levied from airspace users. These corporate entities (most of them publicly owned, but some partly privatized) are now commonly referred to as Air Navigation Service Providers (ANSPs). European states are responsible for providing air traffic services (ATS) as a public service in the sovereign airspace above their respective state territory, while states may delegate part of their airspace to neighboring states for operational reasons. (Baumgartner in Cook, 2016: 10)

In 1960, EUROCONTROL, the European Organization for Safety of Air Navigation was established and its convention revised and broadened in 1997. The organization plays a key role in European Air Traffic Management with a wide range of strategic as well as operational programs, initiatives and bodies. (Baumgartner in Cook, 2016: 11). As an intergovernmental organization, EUROCONTROL is based on its own treaty and not part of the EU family (van Houte in Cook, 2016: 181)

The Single European Sky is an initiative introduced in 1999 by the European Commission, for the reform and defragmentation of Air Traffic Management and adopted in 2004 by the European Parliament and Council. The legislation takes the form of EU regulations. (Van Houte in Cook, 2016: 181)

As part of the Single European Sky regulatory framework, the concept of Functional Airspace Blocks (FABs) was introduced, with the aim of giving ANSPs the responsibility to enable optimum use of airspace. The EU vision for FABs is to gradually adjust from national territory airspace to more functional areas. (Van Houte in Cook et al. 2016: 193)

3.3 Terminology in the ATM domain

Now, let us have a look at the different terms that were used so far (ANS, ATS, ATM, ATC) and see in what way they are related. However, while it is necessary to be aware of these differences in meaning and scope, it should be mentioned that ATM is often used as the generic term when describing the overall domain, in which Air Navigation Service Providers act:

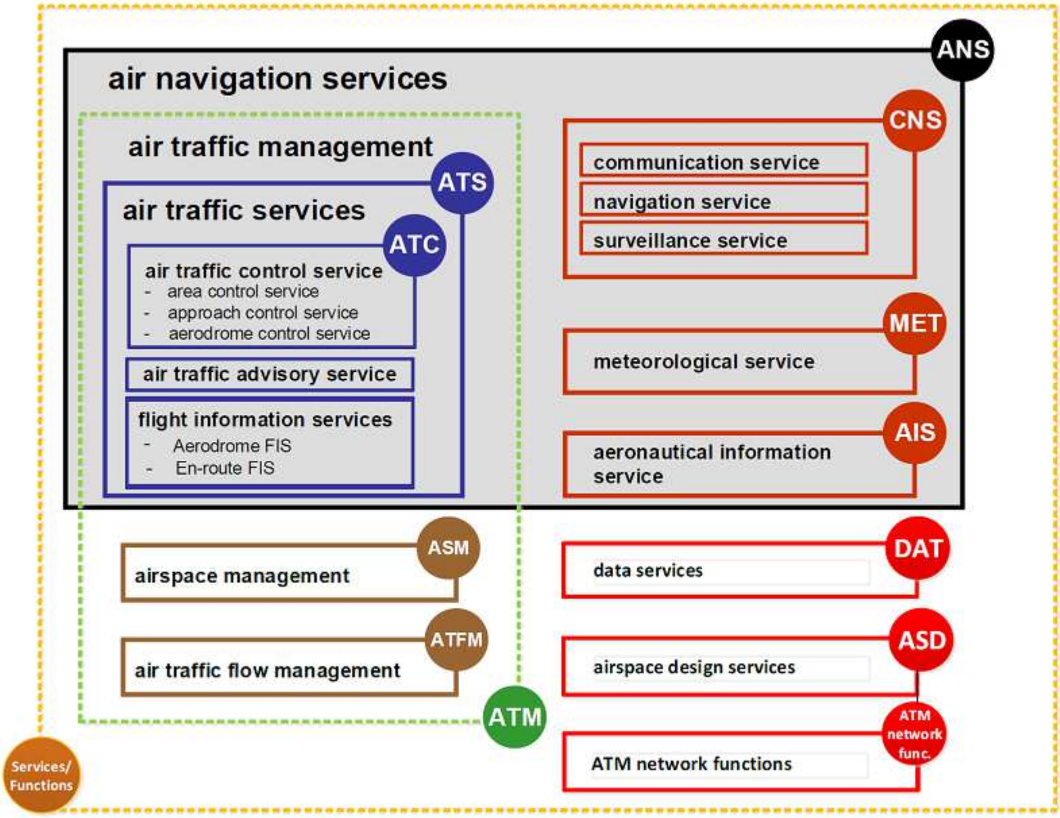

Figure 8: Services in the Framework of Air Traffic Management (EASA, 2018)

Air Traffic Control (ATC): The actual control of airspace on and around aerodromes as well as en-route, in the sovereign airspace of a country, plus potentially delegated airspace, as explained prior.

Air Traffic Services (ATS): ATS comprises ATC as well as flight information and alerting/advisory services

Air Traffic Management (ATM): ATM comprises ATS as well as airspace management (ASM) – i.e. the civil-military coordination of airspace – and air traffic flow management (ATFM) – i.e. the coordination of air traffic flows including potential restrictions.

Communication/Navigation/Surveillance Service (CNS): CNS comprises the provision of pilot-controller (air-ground) as well as controller to controller/other coordination partners (ground-ground) communication, the provision of navigation aids for pilots (e.g. instrument landing systems) as well as the provision of surveillance information to the controller (e.g. radar technology for the exact position detection of an aircraft)

Meteorological Service (MET): MET comprises the provision of meteorological information to aviation stakeholders (air traffic controllers, airports, airspace users)

Aeronautical Information Service (AIS): AIS ensures the information flow necessary for a safe, orderly and efficient air traffic flow.

Air Navigation Services (ANS): ANS comprises ATS, CNS, MET and AIS.

3.4 Air Navigation Services as a System of Systems

Kontogiannis et al describe the ATM System as a *"complex, highly interactive engineering system that involves many organizations and a large number of subsystems and components on board and in the ground."* (2018: 4)

He goes on by listing six discrete control elements which represent the main components of the ATM system:

1. **Procedures and regulations:** The ATM system operates according to international and national legislation (ICAO, EU, EASA and state legislation)
2. **ATCOs:** Air traffic controllers are trained, licensed and responsible for providing ATM services.
3. **Automation systems:** The Controller Working Position which runs special software for providing the ATCO with information related to the position, status and separation of aircraft as well as other support systems.
4. **Communication systems:** Exchange systems for air-ground, ground-ground, and air-air voice and data communications
5. **Navigation systems:** Systems that provide real-time positional information to aircraft in order to support their navigation through airspace.
6. **Surveillance systems:** Technology that provides real-time positional information to controllers for tracking aircraft. (Kontogiannis et al. 2018: 7)

This view however does not acknowledge: The role system operators play (e.g. engineers responsible for the integration and maintenance of the controller working position or navigation systems). To reflect this, point 2. “ATCOs” could be changed to “people”, to include ATCOs, procedure experts, safety staff, engineers as planners integrators, maintenance staff etc.

Point 3 “automation systems” could be represent a very complex component, especially as systems become increasingly integrated and interconnected, so let us have a closer look on which sub-system constitute “automation systems” according to Kontogiannis et al. (2018: 10f.):

1. Controller Working Position (CWP): This represents the work environment and tools used by ATCOs to control air traffic. It is made up of voice and date input devices (such as headsets, telephone, displays, mouse, keyboard) as well as special purpose software for, among others:
    a. communicating with aircraft as well as with other units on ground
    b. monitoring the status of CNS systems
    c. monitoring meteorological data
    d. manage flight progress
2. Decision support systems (DSS): These systems support ATCO decision making and fall into three main categories:
    a. Sequencing managers: These systems provide suggestions for optimal traffic sequencing for instance for departing and arriving aircraft to an aerodrome
    b. Monitoring aids (MONA): These systems assist in the monitoring of tracks and adherence to clearances.
    c. Air Traffic Flow and Capacity Management (ATFCM): These systems provide decision support for flow controllers.

Safety nets are put in place to close a control loop in the provision of ATM services, starting with the issuance of an instruction by an ATCO, the aircraft follows that instruction and aircraft behaviour is then presented on the air situation display of the Controller Working Position. When the prescribed horizontal and vertical separation minima may be infringed in a certain time period, a visual and/or aural warning is given to the ATCO, which enables him to detect and acknowledge the warnings and to intervene accordingly to resolve conflict, which closes the loop.

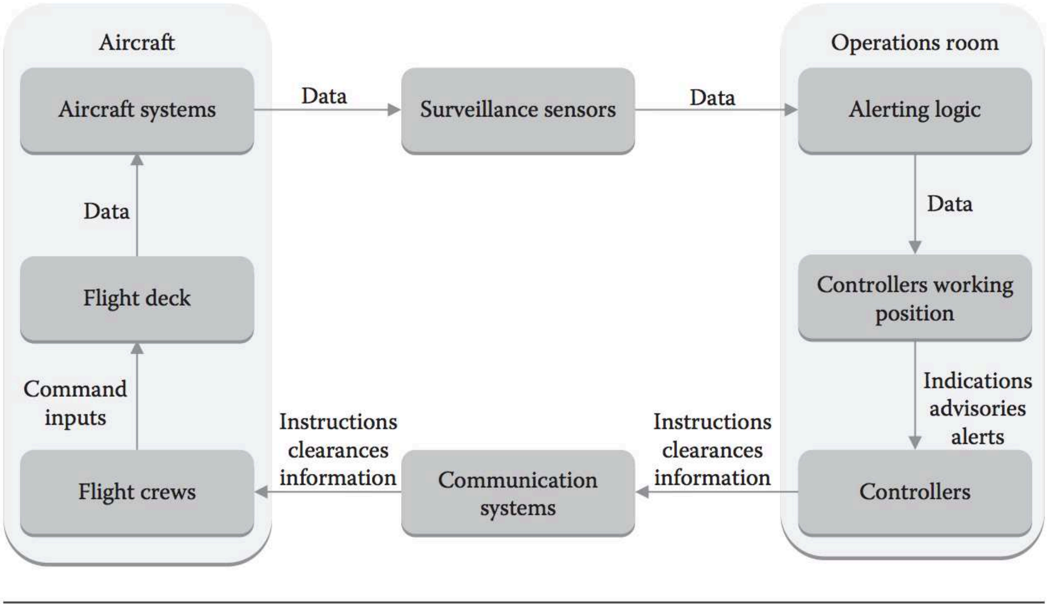

Figure 9: Safety Nets Loop in the ATM System (Kontogiannis et al. 2018:12)

3.5 Uncertainty in ATM

Rivas and Vazquez have identified the following – very disparate – sources of uncertainty in the ATM system:

- **Data uncertainty:** When data is known, but there is a level of uncertainty in their exact values, this type of certainty appears. An example could be an aircrafts position given by a global positioning system (GPS) or an aircrafts performance, based on a simplified aircraft performance model
- **Operational uncertainty:** Human behavior and decision making introduces a degree of operational uncertainty into the system, as it is difficult to predict and can affect, for example, taxi times, departure and arrival times of an aircraft.
- **Equipment uncertainty:** A degraded mode or total equipment failure (e.g. in aircraft or the ATM System) can lead to a system deviating from its normal mode of operation to degraded operation or failure. A loss of communication between air traffic controllers and the pilot of an aircraft

due to communication equipment failure can impact overall traffic efficiency or may even compromise the safe flow of air traffic.

- **Weather uncertainty:** This comprises factors such as uncertain wind conditions, snowfall or temperature. Meteorological predictions only provide likelihoods of certain events occurring. The shorter the time horizon, the more accurate weather predictions become, which means that in the planning stage for flights, routes are only based on estimations that may be very far from reality. (Rivas and Vazquez in Cook and Rivas 2016: 43)

In Chapter 2 of this thesis, the three scales of complex systems where already presented while discussing complex network theory: Microscale, Mesoscale and Macroscale. With the microscale representing a single flight all uncertainty concerning that single flight provides a source for uncertainty for the meso- and macroscale. Within each of the scales, uncertainty leads to two types of problems, a short term horizon and a medium to long term horizon one:

- **Present state estimation:** Data uncertainty is the principle uncertainty source over a short time horizon, during which the main concern is the ability to maintain safety. Uncertainty can be reduced through information sharing and filtering techniques.
- **Future state prediction:** Weather and data uncertainty as well as domino effects propagate over time, so the aim of planning must be the minimization of such effects through optimized system performance (Rivas and Vazquez in Cook and Rivas 2016: 45f)

When studying air traffic under uncertain conditions, flow management presents a difficult problem, as it needs to take into account weather prediction, environmental effects, aircraft trajectories, ground holding and en-route decisions and the propagation of delays into account. The second, more immediate issue is the detection of conflict or the loss of separation between aircraft. (ibid.)

3.6 Safety in Air Traffic Management

Safety, according to the Oxford English dictionary, is defined as *"the condition of being protected from or unlikely to cause danger, risk, or injury"*.

ICAO defines safety as *"the state in which harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management"*.

In this context, we speak of organizational accidents, that may cause danger, risk or injury, not individual accidents. While individual accidents have remained relatively unchanged in nature, organizational accidents, are, as Reason puts it, a product of technological innovations which have strongly impacted and changed the relationships between the human element and technological artifacts in socio-technical systems.

As organizational accidents occur rarely and are hard to foresee, Reasons notes: *"It has been said that nothing in logic is accidental. But does the reverse hold true? Is there nothing logical about accidents? Are there no underlying principles of accident causation?"* – and argues that such principles do indeed exist. (Reasons 2016: 2)

The so-called domino model has been used to examine accident causation, with Heinrich's original model identifying unsafe acts as the key domino, while Weaver et al. focused on the interaction between management omissions and unsafe acts, shifting the main focus of accident prevention onto an organization's management system. (Cooper 2002: 31)

Rasmussen visualizes as safety envelope, created by the boundaries of financial failure (i.e. economic considerations), unacceptable workload (i.e. considerations of efficiency/productivity) and safety failure (i.e. safety considerations):

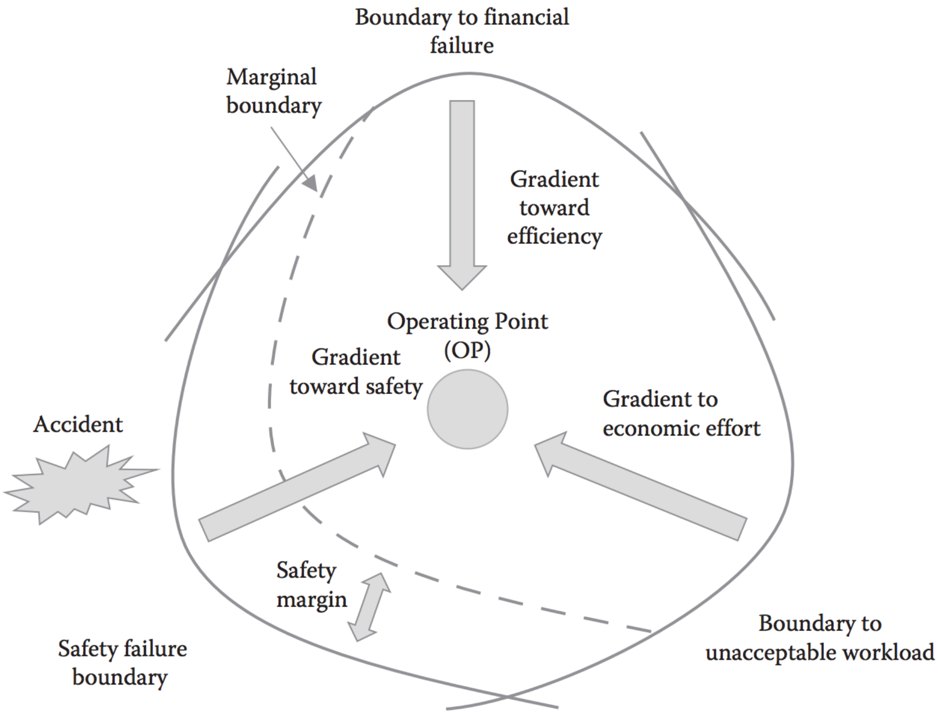

Figure 10: A safety envelope, created by the boundaries of financial failure, high workload and safety failure (Rasmussen in Kontogiannis 2018: 69)

3.6.1 Safety Culture

According to Cooper, the term *safety culture* was first used in the 1987 OECD report on the Chernobyl disaster. In high risk industries (such as aviation is one), safety is likely to be the dominant characteristic of corporate culture, but even in such a primary role, it does not only affect, but is in turn *affected by* organizational systems and operational processes. (Cooper 2002: 30)

An ideal safety culture according to Reason – hard to achieve in the real world, but nevertheless a goal – acts as the engine that propels the system towards the goal of maximum safety, regardless of its leadership's personality or potential economic constraints: *"The power of this engine relies heavily upon a continuing respect for the many entities that can penetrate and breach the defenses. In short, its power is derived from not forgetting to be afraid."* (Reason 2016: 195)

Reason identified the following characteristics as the cornerstones of such a safety culture:

- *Reporting culture:* A safety system depends on the people's (those in direct contact with the hazards) will to participate in it and report relevant information. For this, a reporting culture, which invites the reporting of errors and near-misses needs to be engineered.
- *Just culture:* Reporting culture requires an atmosphere of trust, that encourages or even rewards people for providing essential safety-related information. As just culture does not mean an across-the-board non-blaming culture, a line must be drawn between acceptable and unacceptable behavior (such as non-compliance or sabotage)
- *Flexible culture:* This characteristic of a safety culture points to the ability of high-reliability organizations to reconfigure themselves in the face of danger, switching from the conventional hierarchy to a flatter structure, where control passes to the experts at work and switching back to normal operations once the situation has been dealt with. This adaptability strongly depends on respect for skills, experience and abilities of the people who do the work.
- *Learning culture:* Both the will and the competence needs to be instilled in the people to draw correct conclusions from the information the safety information system provided as well as to implement appropriate reforms when needed.
- Together, these four elements create an *informed culture:* A safety information system shall collect, analyze and disseminate information from incidents and near-misses as well as from regular checks on the vital signs of the system. This data provides knowledge to those who manage and operate the system, about the human, technical, organizational and environmental factors determining the overall system safety. (Reasons 2016: 195f.)

Building on Reason's work, Hudson (2003) defines four organizational components of safety culture:

1. *Safety Values:* Safety is regarded as the license to operate.
2. *Safety Beliefs:* Safety is regarded as commercially feasible and considers accidents as "waiting to happen".

3. *Common Problem-Solving Methods:* Pro-active risk assessments, cost-benefit analyses and search for problems in advance of incidents take place.
4. *Common Working Practices:* Safety is understood as integral to the design and operations and there is a sense of "chronic unease" about safe operations.

Reason suggests that accidents occur when undetected failures, called latent pathogens are associated with active failures and failed defenses by operators. Westrum and Adamski (2009: 77) provide a visualization of these latent failures and active errors in the context of the *human envelope* which, according to their definition comprises learning, decision making, information processing, involvement, adaptability, coordination, training, requisite imagination and resource management.

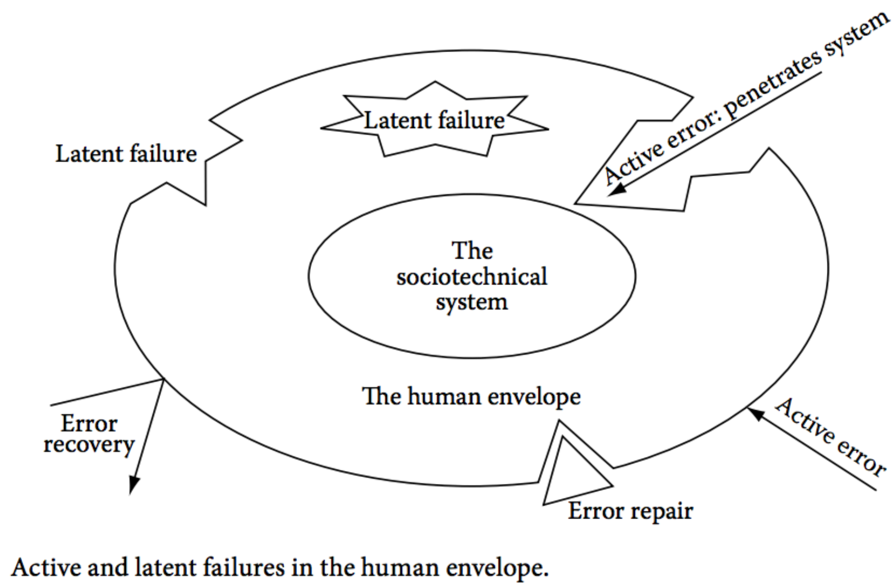

Figure 11: Active and latent failures in the human envelope (Westrum and Adamski in Wise et al. 2009: 91)

Here, Westrum differentiates between three types of organizational cultures and explains their typical behaviors: The pathological, the bureaucratic and the generative. Each type, because of its specific communication pattern breeds different latent pathogens in the human envelope. The more effective the communication, the more latent pathogens can be identified and removed, with the generative type representing the ideal culture, as it is actively and constantly trying to improve itself.

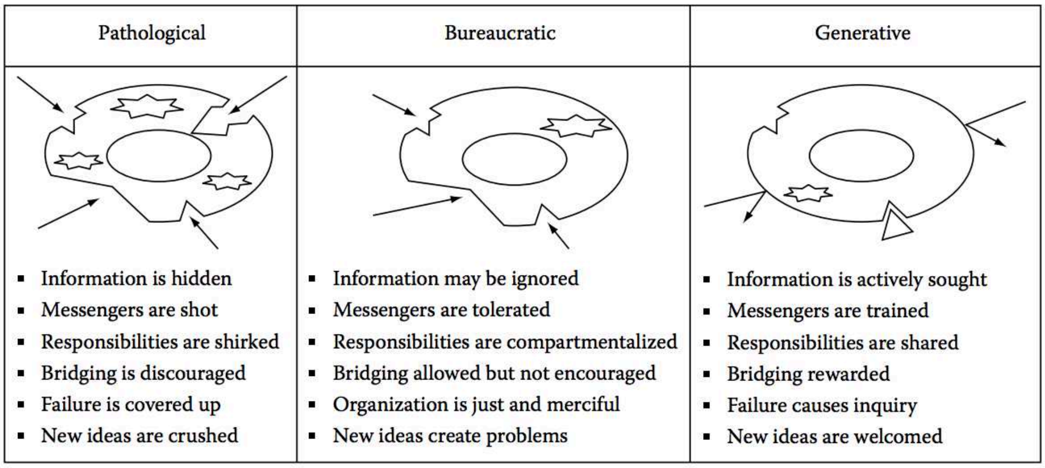

Figure 12: How organizational cultures treat information (Westrum and Adamski in Wise et al. 2009: 91)

However, it is important to point out that according to Schein (1992) no mature aviation organization is ever uniform, as, over a period of time, any social unit will also produce subcultures and this lack of harmony has the potential to erode the integrity of the human envelope. (Westrum and Adamski in Wise et al. 2009: 92f.) While Schein was specifically referring to air crews as social units, I believe this observation is also valid within Air Navigation Service Providers.

3.6.2 A new approach to safety in ATM

In their White Paper on “From Safety-I to Safety-II” Hollnagel et al. advocate for a revised safety approach: They describe the traditional *“Safety-I”* approach as ensuring *that as few things as possible go wrong* and suggests a turn-around into a “Safety-II” approach, the task of which should be to ensure *that as many things as possible go right*. (Hollnagel et al. 2013: 21)

Hollnagel et al. argue this is necessary, as the traditional *Safety-I* view was developed in a time (1960s-1980s) when systems were simpler and more independent and performance demands where lower. In this approach, systems are thought of as decomposable and linear - assumptions, that do not fit today’s reality any more: *"Crucially, the Safety-I view does not explain why human performance practically always goes right. The reason that things go right is not people behave as they are told to, but that people can adjust their work so that ist matches the conditions. As systems continue to develop, these adjustments become increasingly important for successful performance. The challenge for safety improvement is therefore to understand these adjustments, beginning by understanding how performance usually goes right."* (Hollnagel et a. 2013: 3)

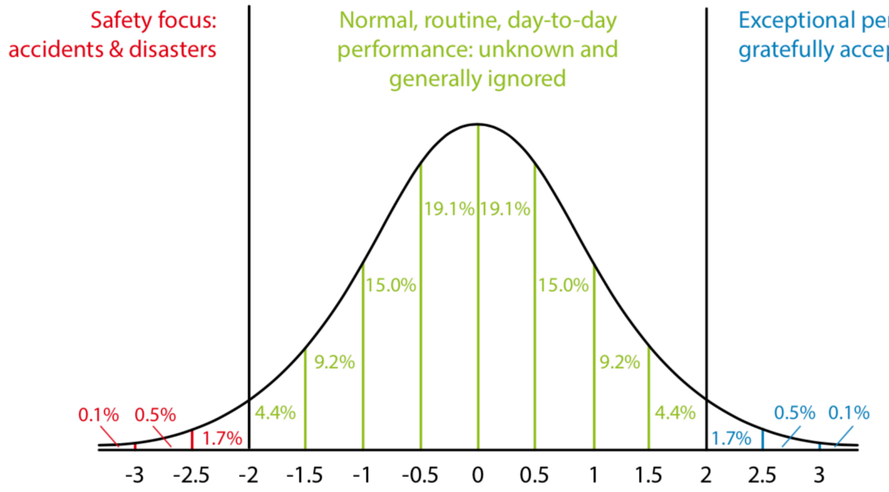

Figure 13: Event probability and safety focus (Hollnagel et al. 2013: 20)

Hollnagel et al. point out how Heinrich's Domino model was based on linear cause and effect relations and a root-cause understanding that cannot be applied to modern-day system complexity any more and explain further, how the principles of functioning of current ATM systems are actually only partly known anymore and systems tend to change at an even faster pace than their description or specification can be completed.

Resilience engineering is explored as a key approach to a new understanding of safety, that acknowledges these increased demands and system complexity as we keep spinning in what Hollnagel calls *"the self-reinforcing cycle of technological innovation":*

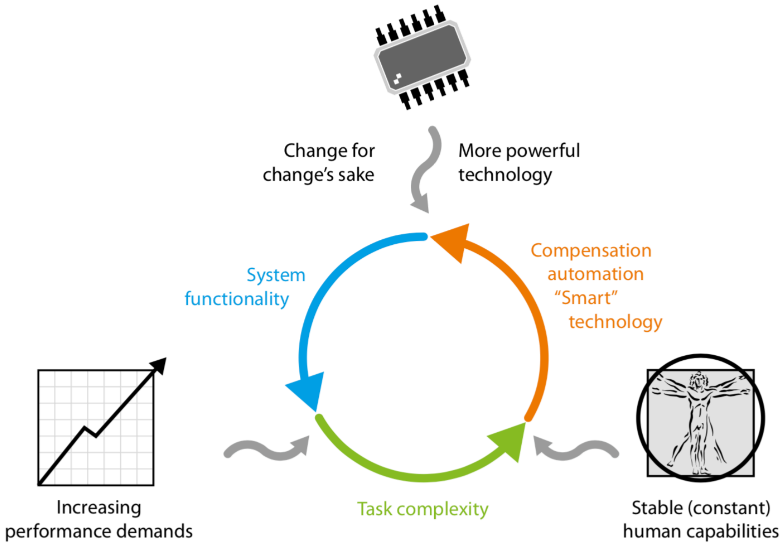

Figure 14: Self-reinforcing cycle of technological innovation (Hollnagel et al. 2013: 13)

Work-as-imagined versus work-as-done

Work-as-imagined describes what should happen under nominal working conditions, whereas work-as-done describes how an concrete work situation unfolds over time. Work-as-imagined is rooted in Taylorism and used as a method to break done tasks and activities in order to improve work efficiency. Applied to safety, this approach meant that in case of an adverse event, system components could be analyzed to identify those that failed and safety could be improved through the careful planning of work, combined with clear instructions and regular training. This approach is built on the belief that procedures and compliance are met in real life *as imagined*.

The work-as-done approach on the other hand acknowledges, that the reality of work differs significantly from how work is imagined to be carried out: *"A practical implication of this is that we can only understand the risks, if we get out from behind our desk, out of meetings, and into operational environments with operational people. […] The way we think of safety must correspond to Work-as-Done and not rely on Work-as-Imagined."* (Hollnagel et al. 2013: 15)

The Safety-II approach therefore propagates the application of the work-as-done concept and instead of asking why or what went wrong (as in Safety-I) it asks why and what went right and how to ensure this is maintained. Hollnagel et al. argue, that instead of treating failures as individual events, they need to be understood as an expression of *daily performance variability*: *"Safety-II is the system's ability to succeed under varying conditions, so that the number of intended and acceptable outcomes (in other words, everyday activities) is as high as possible."* (Hollnagel et al. 2013: 17)

Instead of causality, the concept of emergence should be applied to intractable systems. In the causal thinking of Safety-I, an effect is usually traced back to its root cause, either until the root cause is reached or *until we run out of time or money*, as Hollnagel et al. put it, while in the emergent thinking of Safety-II acknowledges, that a certain effect could be due to transient phenomena/conditions which only ever exist at a particular point in time and space and are do not repeat themselves. (Hollnagel et al. 2013: 19)

So instead of chasing these transient causes, Safety-II sees more value in investing into the understanding, monitoring and management of performance (i.e. how working conditions are created or maintained, which compensate for a lack of time, information or other resources in order to avoid conditions that are known to harm the work). (ibid.)

Having said that, Safety-II is to be seen as a view complementary to Safety-I, rather than a conflicting approach. It is, after all, about the mix but while Safety-I is straight forward in its clarity of a linear root cause thinking, Safety-II is more fuzzy and harder to visualize. Below is a good visualization of why we should pay attention to the daily activities we usually ignore because they work *anyway*:

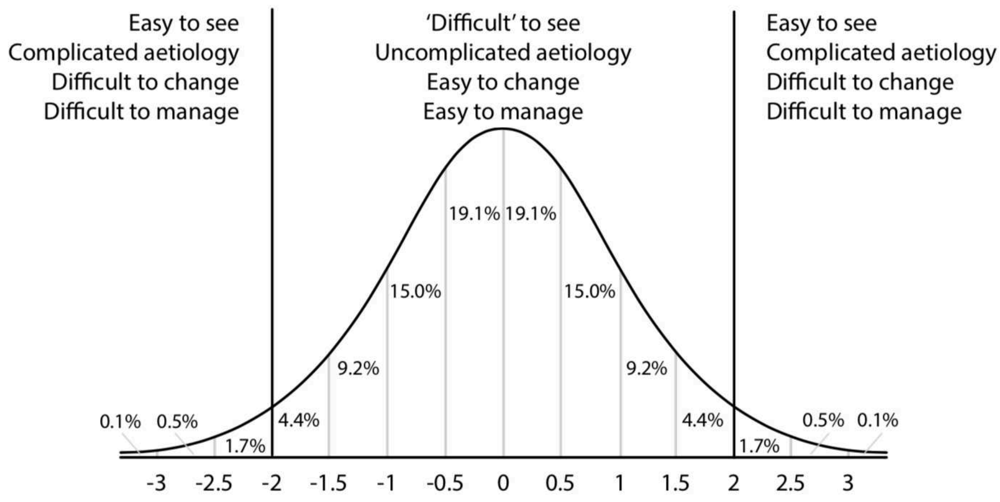

Figure 15: Relation between event probability and ease of perception (Hollnagel et al. 2013: 23)

Hollnagel et al. argue that, instead of focusing on severe events that are unpredictable due to our constantly changing environment, focus should be put on regular events, as they are not only easier to manage, but also easier to change. Of course, this must be done while still remaining sensitive to the possibility of failure.

3.7 Chapter Summary

This chapter has provided a brief history of the development of ATM in Europe, explained relevant terminology, elaborated a system of systems view and discussed the role of safety as well as the need to further develop present-day safety culture in in the light of rising system complexity with a stronger focus on work-as-done, instead of solely looking at work-as-imagined.

4 Research Process

4.1 Introduction

In this chapter, the research process is broken down and reflected upon and the methodology chosen is described.

The research was carried out as a three-step-process:

1. Execution of a *literature analysis* which provides the theoretical framework for the case study.
2. Realization of a *case study* to generate a data corpus aimed at answering the leading research questions.
3. Formulation of a *synthesis* based on the empirical results and the theoretical work.

The purpose of the *literature analysis* was to identify key concepts related to systems theory and complexity as well as to portray the key properties of the Air Traffic Management as a complex system and the central role of safety culture with said system. Chapters 2 and 3 of this work constitute the outcome of this work and provide a framework for the case study.

The *case study* was conducted in the Austrian Air Navigation Service provider. Data was collected in through the participation in various meetings, from meeting notes, working papers, decision papers, project planning documentation as well as a few brief open-ended interview sessions over the course of six months (09.2019 to 02.2020) and analyzed in a qualitative fashion.

The *synthesis* presents and combines empirical outcomes from the case study with the theoretical grounding established in the literature analysis.

4.2 Methodology

This work choses an adaptation of *Grounded Theory* for the process of data collection, analysis and interpretation. Grounded theory is a method rooted in data directly and defines itself an abductive mechanism, meaning it is used for deriving hypotheses. Whereas inductive methods draw conclusions from the usual to the general, abductive methods aim at forming a hypothesis about a case, *through* the analysis of a case. Developed by Glaser and Strauss in the 1960s, Grounded Theory is built and (temporarily) confirmed through the systematic collection and analysis of data, that relate to the phenomenon under examination, meaning that data collection, analysis and theory stand in a reciprocal relation to one another. It is therefore, according to Strauss and Corbin (1998) not an initial theory, waiting to be confirmed, but instead a problem field, whose pertinent issues will be revealed through the research process. Grounded theory is, essentially, not a theory, but a method for theory development, anchored in the interactionist paradigm of Mead and Blumer (Weszelits 2010).

The following assumptions of grounded theory developed on the basis of an interactionist perspective:

- If you want to understand what is going on, you need to enter the field
- Theories anchored in reality contribute to the development of professional disciplines
- The nature of experience and acting develops and changes constantly
- Humans play an active role in the shaping of the world, they live in
- The process-like and complex nature of life needs to be highlighted
- There is a connection between condition, meaning and acting. (Strauss and Corbin 1996: 9)

Theoretical sampling is a central principle of grounded theory: In the process of data collection, which aims at generating explanatory hypotheses, the researcher collects, codes and analyses in iteratively, deciding step by step which data to collect next. The selection needs to correspond to the theoretical relevance for the research topic. It is therefore not a statistically representative sampling (which can only be achieved through random selection), but a sampling, which facilitates the criteria of minimal and maximal contrast of data within the established data corpus. According to Strauss and Corbin (1996: 150) as well as Keller (2007: 109), theoretical sampling guarantees the tracing of variation, process and density and it is important to not chronologically separate the process of data collection, coding and analysis in in subject-anchored research. (Strauss and Corbin 1996: 148-165)

Apart from the concept of theoretical sampling as explained above, the coding process as a methodological approach is at the heart of grounded theory. This study follows Keller's suggestion of a "loose" orientation on the coding process: The first step is an open coding, at which the compiled data are broken down, examined and categorised. (Strauss and Corbin 1996: 43f.) The text fragments get broken down into individual fragments, which receive codes to describe their characteristics. Codes are never final and may therefore change during the process. Once all fragments relevant to the research questions have been coded, fragments are grouped into superordinate codes, whose frequency will sheds light on their relevance in the overall research area.

4.3 Data Compilation

Data was compiled from the following sources:

1. *Meetings*: This source provided the biggest share of data in the overall compilation. The following meetings were considered:
    a. *Strategic ANS planning meeting (3 sessions)*
    b. *ANS Requirements Consolidation Meeting (6 sessions)*
    c. *Change Advisory Board Meeting (6 sessions)*
    d. *System Architecture Board Meeting (10 sessions)*
2. *Various internal documents*: Working papers, decision papers, project planning documentation, safety documentation.
3. *Open ended "flash"-interviews* with requirement engineers, integrators and managers of the company who are involved in the management, planning and integration of system changes (seven flash interviews in total):
    a. These interviews were of very short nature and usually done on the sidelines of the above meetings.
    b. The purpose of these flash interviews was to elaborate further on topics discussed in the meetings as well as to collect *sentiment*.

Access to these meetings and documents was granted through my role of System Architecture Manager in the Engineering Department of the Austrian Air Navigation Service Provider.

4.4 Benefits and limitations of the research approach

The benefits of the research approach can be summarized as follows:

- *Access:* Access to a large pool of data that would otherwise not be accessible for research as well as to a relevant network of experts and managers
- *True-to-life:* Experience and expert knowledge allows for the formulation of targeted research questions, which address an actual real life problem in the field.

The limitations of the research approach can be summarized as follows:

- *Confidentiality:* Apart from the quotes included in the results chapter, the documentation used is confidential due to the internal nature and can therefore not be published as an annex to this work.
- *Focus/reduction:* Findings that are valid for one Air Navigation Service Provider might only have limited validity for other Air Navigation Service Providers. A clear identification of surrounding conditions (environmental analysis) is therefore crucial.
- *Some untapped consolidation potential:* The research conducted is of clear explorative nature, leaving some consolidation potential unaddressed as a result of the general set-up chosen.

4.5 Chapter Summary

The nature of the research questions rendered a qualitative research approach suitable, building on a set of data composed of meeting notes, working papers, decision papers, project planning documentation as well as short open-ended interviews. The collected data yields the coding results as presented in the succeeding chapter.

5 Results

5.1 Introduction

Before proceeding with the presentation of the coding results, the first part of the chapter will deliver relevant background information about the organization, at which the study was conducted.

5.2 Background and context

The Austrian Air Navigation Service Provider is a government limited liability company with a little over 1000 employees, whose key task is to maintain a safe, punctual and efficient air traffic flow in Austrian (as well as delegated) airspace, 24/7 throughout the year.

The company received its Single European Sky certification in 2006 and is entitled to provide air traffic services throughout the European Union. The organization operates one Area Control Center in Vienna as well as six Towers in Vienna Schwechat, Salzburg, Innsbruck, Linz, Graz and Klagenfurt (from where Tower and Approach Control Services are provided). The engineering department of the organization operates all infrastructure required for operations (Surveillance, Communication, Navigation Systems, Meteorological Systems and the overall Air Traffic Management System of Systems).

For systems development all Air Navigation Service departments of the company (i.e. the Air Traffic Management department, the Engineering department as well as the Meteorological department) collaborate in a number of expert groups and management boards under the inclusion of safety peers.

5.3 Coding results

As explained in chapter 4 the data compilation was analyzed and categorized into codes. The most relevant (i.e. most frequently allocated codes) are described in detail in this section.

5.3.1 The unknown unknowns

"We must work on the reduction of the unknown unknowns."

This statement, or variations thereof, come up frequently when discussing system changes. The underlying assumption is, that unknown unknowns always exist in a system in a latent fashion, that may never cause a problem if the system remains unchanged. However, when a parameter in a system is changed or a new function is introduced, the unknown unknowns may cause an undesired effect. This issue was already touched upon in the discussion of Safety-II as a concept that acknowledges, that systems have long outgrown their specifications, because documentation simply cannot keep up. At the end, the fear of the unknown unknowns becomes a question of liability: If a change causes an unknown unknown to generate a negative effect, who will be liable and will the reason, the change was made after all, justify a potentially adverse outcome?

This is also connected to a concept described as the "grandfather principle": Old rules continue to apply to some existing situation, while new rules only apply to future cases. *"But once you start digging, you will certainly find deficiencies in existing situations"*.

5.3.2 Dynamics of the environment

"Environment dynamics are a heavyweight factor in the planning of changes."

There are a number of environmental factors, that dynamically change and thereby impact the planning and implementation of changes into the ATM system and that may create domino effects. To give some examples:

- The replacement of an old secondary surveillance radar infrastructure with a modern mode-s radar, depends, among others, on the receipt of a building permit. This lengthy bureaucratic approval process could significantly delay the schedule to a point where other interrelated projects are impacted or to a point where the old radar can no longer be operated for end of life reasons. While safety is always ensured through a multilayer surveillance system as well as through procedures that cover various failure modes, these delays tie resources of the project manager and others.

- A regulatory requirement might pop up with not enough lead time to implement it. An example for this is the recently imposed "requested flight level adherence", which asks ANSPs to only clear aircraft to the flight levels they filed in their flight plan per segment. This is a sensible requirement in principle, as it ensures that flow management measures are actually able to take effect. However, there is a catch: Most ATM systems in Europe are not able to show the last filed flight level to the ATCO in a specific segment between waypoints, once a direct has been given that overrides the initial route. Which leads us to the next topic:

5.3.3 "Quick and dirty" solutions that become permanent

The pressure to act often provokes the necessity of finding a quick solution to a specific problem (such as the one described above). Due to the inertia of the stable architectures that carry the overall system, quick solutions are usually found "off the beaten track". While the initial aim is usually to replace those quick solutions with proper solutions when possible, organizations tend to end up keeping a growing number of skeletons in the closet (cue: *work-as-done*), that the overall system needs to support.

5.3.4 Emergence

"I can't tell you what I want, before I have seen all possibilities there are."

This is an expression commonly raised by Air Traffic Controllers as system users during the requirements definition for a certain change. Emergence and emerging functions of systems were already discussed in detail in the context of systems theory and safety culture. Emerging applications of system functions have a long history. It is often, that new possibilities of application are discovered, once a new system or technology is put into operation for an entirely different reason. One striking example is Mode-S technology. Originally, the idea behind Mode-S secondary radar technology (s stands for selective) was to reduce "all call" surveillance radar interrogation rates through selective interrogations of single aircraft. However, the downlinked parameters provided by aircraft through Mode-S technology provided not only useful for position identification of aircraft, but also for meteorological data (since aircraft also downlink their sensor measurements for wind etc. through Mode-S). Now, a lot of meteorological systems use Mode-S data as a foundation for weather services. While this is an excellent example of emergence, it is also a great input for the next topic:

5.3.5 System limits

An issue, when implementing changes and additional functions in the ATM system are system limits or bottlenecks. The above mentioned Mode-S usage for meteorological services for example contributes to the transponder interrogation overload currently experienced in Europe. Since interrogations in some areas in European areas now by far exceed the transponder limits as specified by ICAO, a sudden loss of surveillance coverage has become a real risk. European Air Navigation Service Providers are therefore now starting to work on potential solutions together. Until a solution is found, any emerging application of for example Mode-S data (that does not serve the main function of position identification) have to be cut back. Another example are ATM system processing limits: While a wider surveillance horizon is desired by ATCOs for planning reasons (for early identification of future traffic) the system has upper processing limits, that might not allow for the full desired planning horizon.

5.3.6 Vendor lock-in and partnership issues

ANSPs depend hugely on their relations with industry partners. First of all, it is a specialized market with limited competition, leading to a few big players controlling the market. This is due to the fact that the development and sustainment of ATM systems is a voluminous and capital-intensive endeavor, that does not really allow for a "start-up culture". Whenever partnerships are contracted, their time horizon is usually measured in decades. The same is valid for partnerships between ANSPs. While there are many upsides to stable relations, there are also undesired effects, which usually surface when contrarian interests meet. When an individual interest of one organization in a partnership is not met by others, this can cause an organization to feel locked-in and immobile and it can make certain changes impossible or delay them.

5.3.7 Maturity

In ATM, maturity of solutions is an issue, leading to situations, were certain solutions are required through regulation, that will not have reached maturity by the time they are mandated. This is an issue known to regulatory bodies and has recently lead to the shifting of implementation deadlines, such as for the implementation of time based separation (as opposed to distance based separation) on major European aerodromes.

5.3.8 The thin line between safety and capacity

The relevance of safety considerations in ATM has been outlined in chapter 3. While there is agreement on the fact, that ensuring safe operations is the paramount priority in ATM, it is often discussed, whether or not a certain change is safety-relevant or not. There is even a common expression, referring to someone applying the "safety cub" in order to enforce certain interests. While it is certainly not appropriate to trivialize safety requirements, an organization needs to exercise care in not using safety as an argument, where it isn't one. For example: The non-availability of a certain function could lead to reduced capacity, while still maintaining required safety levels.

5.3.9 Airborne equipage

Some changes in the ATM system depend on airborne equipage, such as – for example – ADS-B transponder equipment. Without a sufficient number of aircraft equipped, an implementation on ground is of little use, sometimes leading to chicken or the egg causality dilemma, with neither party willing to be the first mover for financial reasons. Which brings us to the next topic:

5.3.10 Cost-benefit-analysis issues

With certain requirements, it is hard or even impossible to assess, whether the benefit of a change will outweigh its cost. Stranded cost is another issue that ANSPs have to sensibly deal with in their economic responsibility towards airspace users, whose charges are impacted by ANSPs investments.

5.3.11 Dynamic needs and fuzzy requirements

In the process of pinning down and accurately describing requirements for a system change or new system, the issue of dynamic needs and unclear requirements arises.

When not dealt with, this can lead to stranded cost, when an unclear case for action is taken to far. At the same time, it needs to be understood, that requirements are hardly ever born "perfect", they need to be developed and there needs to be room for development. This is an issue, which strongly interacts with the next topic:

5.3.12 Perpetuation of operations beats improvement

This conflict is a slippery slope, kicked off by resource bottlenecks. In certain situations, where the effort to implement requirements exceeds the resources available for the cause, prioritization becomes a necessity. With the CBA issues explained above, this becomes an unpopular task. If no decision is made, the rule is *"perpetuation of operations has priority"*. In order to not arrive at a deadlock at some point, this conflict needs to be solved.

5.3.13 Safety in the context of system changes

In accordance with EU Regulation 2017/373, the organization defines its Safety Management System (SMS) as *"a systematic approach to managing safety, including the necessary organizational structures, accountabilities, policies, and procedures."*

The organization's SMS foresees the conduction of a safety support assessment for each relevant change. While it is the responsibility of the change owner, trained Safety Assessment Peers are provided as support. The change owner is defined as person responsible for the implementation of the change. There is no indication, that this change owner may shift as the change process advances (e.g. from the initial requestor to the requirements engineer to the project manager to the integrator). The safety process supports the system lifecycle transversally, with a hazard analysis, the provision of safety criteria, safety requirements, safety support requirements as well as a documented safety case.

The SMS acknowledges, that the organization's management system or its sub systems may have an (latent) impact on the functional systems. This includes changes in organization, personnel, strategic decisions and mechanisms for the provision of resources, modification of company culture, goals, management methods etc. However, there is no specific focus or detail on the requirements engineering process or the concept phase of a change.

5.4 Chapter Summary

The findings extracted from the collected data show how the management of change and system development is susceptive to a number of system-internal as well as external influencing factors, as well as how decision making challenges appear as a central aspect of system development. The succeeding chapter will confront the findings with the research questions formulated in chapter 1.

6 Discussion of Findings and Outlook

6.1 Introduction

The closing chapter of this thesis is dedicated to the discussion of the study findings in the light of the research questions, as well as to delivering suggestions for further research.

6.2 Research Findings

The findings presented in chapter 5 have yet to be confronted with the research questions RQ1 and RQ2, which were presented in chapter 1 as guidance for the literature review and the study:

RQ1: What are the main internal and external drivers of complexity into Air Traffic Management System Architecture and what are their (potentially reciprocal) effects?

RQ2: In what ways has Safety Culture (relevant Regulation as well as internal measures) responded to increased organizational and system complexity and how is this factored (or not) into the requirements engineering process?

RQ1 can be answered as follows:

There are various internal and external drivers of complexity into ATM System Architecture that have strong reciprocal effects:

- Dynamics of the system environment, including regulations that act as moving targets
- Overall system limits which need to be considered
- Pressure to act quickly, which leads to solutions that do not conform with overall system architecture principles
- The fuzziness of requirements as well as the unpredictability of exact outcomes
- The fuzzy line between safety and capacity considerations
- Dependency on airborne equipage, on industrial readiness as well as on the actions of other ANSPs

ATM system development navigates in a very volatile space. While some of these complexity drivers are external and cannot be controlled, there are some internal factors worth tackling from a perspective of improving organizational efficiency. Also, the results indicate a strong need of strengthening decision making power as well as providing decision making support tools in the requirements engineering phase of the change, as it is there, where the kind of errors occur which require the highest effort to correct in later stages. The considerations of the Safety-II approach that focuses on work-as-done could also be of value to the change management process.

The table below presents a mapping of the most relevant findings to RQ1:

Driver	**I/E**	**Summary Description**	**Evi-dence**	**Implications**
1. Emergence	Internal	In multifunctional, complex systems a change or additional function will often lead to usages outside the initial core requirement.	5.2.4	Requirements engineering and ATM system architecture need to be more aware of these emergent effects and factor them in to a defined extent. Reciprocity with: 4. (emergent uses may lead to additional bottlenecks); 5. (emergent uses may lead to additional requirements)
2. Dynamic Environment	External	There are a number of environmental factors, that dynamically change and thereby impact the planning and implementation of changes into the ATM system and may create domino effects.	5.2.2 5.2.7 5.2.9	Risk management needs to take place increasingly not just on a project management level, but also on a *programme* management level. Reciprocity with: 3. (environmental dynamics and deceleration through partnership complexity may create a field of conflict); 4. (dynamic external requirements may put additional stress on existing bottlenecks)

3. Partnership Dependencies	External	ANSPs depend on long-term relations with industry partners as well as with other ANSPs. These partnerships drive complexity into the system, as partnerships need to consider and reflect the interests and requirements of all involved parties.	5.2.6 5.2.9 5.2.12	Complexity issues need to be recognized and dealt with on partnership level. Reciprocity with: 2 (see above); 4 (the resolution of system bottlenecks depends on the capabilities of the partners to do so)
4. Bottlenecks	Internal	Technical system bottlenecks as well as resource bottlenecks increase system complexity, e.g. through the implementation of workarounds.	5.2.3 5.2.5 5.2.12	An early warning system for bottleneck detection needs to be factored into the change planning and decision process. Reciprocity with: 1. (q.v.), 2 (q.v.) ; 3 (q.v.) ; 5. (volatile requirements could worsen existing bottlenecks)
5. Volatility/ variety/ number of requirements	Internal	The number, variety and volatility of requirements boost complexity. With certain requirements, it is hard or even impossible to assess, whether the benefit of a change will outweigh its cost. In some cases, it is hard to assess whether a certain requirement is a safety or a capacity requirement.	5.2.10 5.2.11	A stable decision support framework for requirement prioritization needs to be put in place. Reciprocity with: 1. (q.v.); 4. (q.v.); 6. (volatile requirements could create preventable unknown unknowns)
6. Uncertainty/ Unpredict-ability	Internal	Unknown unknowns always exist in a system in a latent fashion, that may never cause a problem if the system remains unchanged. However, when a parameter in a system is changed or a new function is introduced, the unknown unknowns may cause an undesired effect.	5.2.1	A human factors perspective on manageable levels of technical complexity needs to be established. Reciprocity with: 4. (q.v.)

Table 5: Summary of Findings for RQ1: Main internal and external drivers of complexity into Air Traffic Management System Architecture and (Reciprocal) Effects

RQ 2 can be answered as follows: While the organization manifests a strong Safety Culture that delivers an above average safety level, there has been no specific response towards increased system or organizational complexity beside the incorporation of EU IR 2017/373 considerations concerning the change process. The safety guidelines for change management start at the concept level and not already at the inception of a need, meaning that the initial requirements engineering process receives no *targeted* safety guidance. Overall, the safety approach can be described as still mostly following the linear Safety-I concept, meaning that there is potential to examine potential benefits of the Safety-II concept as an extension.

The table below presents a mapping of the findings to RQ2:

Safety Culture Aspects	**Response to increased system complexity**	**Evi-dence**	**Implications**
Regulation (external)	EU Regulation 2017/373 puts stronger focus on system changes, requiring an update of the change management process for the regulator to be informed on any changes of the functional system. However, this does not automatically ensure specific safety focus in the requirements management phase of a change.	5.2.13	ATM Regulation could benefit from increased appreciation of the complexity drivers which impact/limit the room for manoeuver of ANSPs.
Organi-zation (internal)	Internal procedures have been updated to reflect regulatory requirements, they do however provide a transversal function with no specific focus on the requirements management and system architecture definition phase.	5.2.1 5.2.5 5.2.8 5.2.13	The organization could benefit from an increased focus of safety culture on the initial phases of the change management process, supporting a clear differentiation of safety requirements versus capacity requirements. Safety-II considerations could be factored in, to reflect the non-linearity of current systems behavior.

Table 6: Summary of findings for RQ2: Safety Culture in the face of increased system complexity

6.3 Outlook

The purpose of this study was to generate a better understanding of how complexity impacts system development in Air Traffic Management. The exploration of system development in the light of system complexity revealed a number of research paths worthy of further exploration: Further research could widen the initial argument with a study that looks at and analyzing similarities and differences between various Air Navigation Service Provides in Europe. Also, a closer look could be taken at the role automation plays and will continue to play as ATM systems mature and how safety culture might need to further adapt to these developments. As the results of the study show a strong connection between Requirements Engineering and decision making processes, a deepened exploration of this relation seems highly relevant for further research as well as application.

References

- Alenljung, Beatrice (2008): Envisioning a Future Decision Support System for Requirements Engineering – A Holistic and Human-centered Perspective. Linköping: Dissertation 1155.
- Cook, Andrew and Rivas, Damián (2016): Complexity Science in Air Traffic Management. New York: Routledge.
- Cook, Andrew et al. (2016): European Air Traffic Management. Principles, Practice and Research. London and New York: Routledge.
- Cooper, Dominic (2002): Safety Culture. A model for understanding & quantifying a difficult concept. Published in: Professional Safety, June 2002.
- Crawley, Edward et al. (2016): System Architecture, Strategy and Product Development for Complex Systems.
- Dick, Jeremy et al. (2017): Requirements Engineering. Cham: Springer.
- Ebert, C. and Wieringa, R.J. (2005): Requirements engineering: Solutions and trends. In: Aurum and Wohlin (Eds.) Engineering and managing software requirements (453-476). Berlin: Springer-Verlag.
- Garnsey, Elizabeth and McGlade, James (2006): Complexity and Co-Evolution.
- Geels, Frank W. (2005): Technological Transitions and System Innovations. A Co-Evolutionary and Socio-Technical Analysis
- Strauss, Anselm and Corbin, Juliet (1996): Grounded Theory: Grundlagen Qualitativer Sozialforschung. Weinheim: Beltz/PVU.
- Haberfellner, Reinhard et al. (2015): Systems Engineering, Grundlagen und Anwendung. Zürich: Orell Füssli.
- Haberfellner, Reinhard et al. (2019): Systems Engineering, Fundamentals and Applications. Munich: Birkhäuser.
- Hammel, Christian et al. (2008): Anwendung von Methoden aus der Theorie Komplexer Netzwerke für die Optimierung der Layouts von MFS. 4. Fachkolloquium der Wissenschaftlichen Gesellschaft für Technische Logistik e. V.

- Hollnagel, Erik et al. for the Network Manager/Eurocontrol (2013): From Safety-I to Safety-II: A White Paper. Brussels: Eurocontrol.
- Hood, Colin et al. (2008): Requirements Management. The Interface Between Requirements Development And All Other Systems Engineering Processes. Berlin, Heidelberg: Springer-Verlag.
- Hudson, Patrick (2003): Safety Management and Safety Culture. The Long, Hard and Windign Road. Leiden University: Paper.
- Karafyllis, Nicole C. "Soziotechnisches System" in Liggieri, Kevin und Müller, Oliver (2019): Mensch-Maschine Interaktion. Berlin: J.B. Metzler
- Keller, Reiner (2007): Diskursforschung. Eine Einführung für SozialwissenschaftlerInnen. Wiesbaden: Verlag für Sozialwissenschaften.
- Kohr, Dominik et al. (2017): Identifying Complexity Drivers in Discrete Manufacturing and Process Industry. In: Procedia CIRP 63, 52 – 57
- Kontogiannis, Tom and Malakis, Stathis (2018): Cognitive Engineering and Safety Organisation in Air Traffic Management. Boca Raton: CRC Press.
- Krizanits Joana (2015) Der Tanz mit der Komplexität: Tools für Teams. Zeitschrift für Unternehmensentwicklung und Change Management. – Düsseldorf. Vol. 34. 42-48.
- Kuhn, Thomas S. (1967): Die Struktur wissenschaftlicher Revolutionen. Frankfurt a. M.: Suhrkamp.
- Mallikarjan, Jagadish Thimiri and Smith, Eric (2015): Synergy and Emergence in Systems Engineering. Conference Paper for a System of Systems Engineering Workshop. Albuquerque.
- Maté, Louis Jose and Silva, Andrés (2005): Requirements Engineering for Sociotechnical Systems. Hershey, Melbourne, London, Singapore: Information Science Publishing.
- Meyer, Christian (2007) Integration des Komplexitätsmanagements in den strategischen Führungsprozess der Logistik. Haupt: Bern.
- NASA (2007): NASA Systems Engineering Handbook.
- Orasanu, J. and Connolly, T. (1993) The reinvention of decision making. In: G.A. Klein, J. Orasanu, R. Calderwood and C.E. Zsambok (Eds.): Decision

making in action: Models and methods (pp 3-20). Norwood, New Jersey: Ablex Publishing.

- Perrow, Charles (1984). Normal accidents: Living with high-risk technologies. New York: Basic Books.
- Piya, Sujan et al. (2017): Supply Chain Complexity Drives and Solution Methods. in: Int. J Sup. Chain. Mgt Vol. 6, No. 4, Dec 2017
- Reason, James (2016): Managing the risks of organizational accidents. New York: Routledge.
- Reymondet, Lucie (2016): A framework for sense-making of complex sociotechnical systems. Massachusets Institute of Technology: Master Thesis.
- Seife, Charles (1999): They have a problem. New Scientist, No. 2218, 14.
- Seradarasan, Seyda (2013): A review of supply chain complexity drivers. In: Computers & Industrial Engineering. IOS Press.
- Shafiee, Sara et al. (2019): Development of a Design- ime Estimation Model for Complex Engineering Processes. In Hiekata et al. (Eds): Transdisciplinary Engineering for Complex Socio-technical Systems.
- Sheard, Sarah and Mostashari, Ali (2010): A Complexity Typology for Systems Engineering. ICOSE International Symposium: Paper.
- Shorrock, Steven et al. for the Network Manager/Eurocontrol (2014): Systems Thinking for Safety: Ten Principles, A White Paper.
- Vogel, Wolfgang and Lasch, Rainer (2016): Complexity drivers in manufacturing companies: a literature review. In: Logist. Res.
- Weszelits, Anna (2010): Die wissenschaftliche Publikationspraxis als Reproduktionsort hegemonialer Diskursstrukturen. University of Vienna: Master Thesis.
- Wise, John et al (2009): Handbook of Aviation Human Factors. Boca Raton: CRC Press.
- Woods, David D. and Hollnagel, Erik (2006): Joint Cognitive Systems. Patterns in Cognitive Systems Engineering.
- Woods, David D. and Hollnagel, Erik (2005): Joint Cognitive Systems. Foundations of Cognitive Systems Engineering. Boca Raton: CRC Press.

List of figures

FIGURE 1: ASPECTS OF A SYSTEM (HABERFELLNER 2019: 10) 7

FIGURE 2: THE SELF-REINFORCING COMPLEXITY CYCLE (WOODS AND HOLLNAGEL 2005: 4) 16

FIGURE 3: CONTRIBUTORS TO AND EFFECTS OF COMPLEXITY (SHEARD 2010: 936) 17

FIGURE 4: LIFE-CYCLE COST IMPACTS FROM EARLY PHASE DECISION-MAKING (NASA 2007: 13) 21

FIGURE 5: SHARE OF ERRORS IN REQUIREMENTS IN TOTAL NUMBER OF ERRORS (HOOD ET AL. 2008: 13) 22

FIGURE 6: REQUIREMENTS ENGINEERING PROCESS (ALENLJUNG 2008: 17) 24

FIGURE 7: REQUIREMENTS MANAGEMENT (ALENLJUNG 2008: 29) 25

FIGURE 11: SERVICES IN THE FRAMEWORK OF AIR TRAFFIC MANAGEMENT (EASA, 2018) 36

FIGURE 12: SAFETY NETS LOOP IN THE ATM SYSTEM (KONTOGIANNIS ET AL. 2018:12) 39

FIGURE 13: A SAFETY ENVELOPE, CREATED BY THE BOUNDARIES OF FINANCIAL FAILURE, HIGH WORKLOAD AND SAFETY FAILURE (RASMUSSEN IN KONTOGIANNIS 2018: 69) 42

FIGURE 14: ACTIVE AND LATENT FAILURES IN THE HUMAN ENVELOPE (WESTRUM AND ADAMSKI IN WISE ET AL. 2009: 91) 44

FIGURE 15: HOW ORGANIZATIONAL CULTURES TREAT INFORMATION (WESTRUM AND ADAMSKI IN WISE ET AL. 2009: 91) 45

FIGURE 16: EVENT PROBABILITY AND SAFETY FOCUS (HOLLNAGEL ET AL. 2013: 20) 46

FIGURE 17: SELF-REINFORCING CYCLE OF TECHNOLOGICAL INNOVATION (HOLLNAGEL ET AL. 2013: 13) 47

FIGURE 18: RELATION BETWEEN EVENT PROBABILITY AND EASE OF PERCEPTION (HOLLNAGEL ET AL. 2013: 23) 49

List of tables

TABLE 1: EXTERNAL AND INTERNAL COMPLEXITY DRIVERS IN MANUFACTURING (AS IDENTIFIED BY KOHR ET AL. 2017: 55) 19
TABLE 2: EXAMPLES OF NETWORK PROPERTIES ACROSS MULTIPLE DOMAINS (COOK AND ZANIN IN COOK AND RIVAS, 2016: 11) 31
TABLE 3: INTRODUCING NETWORK SCALES (BASED ON COOK AND ZANIN IN COOK AND RIVAS, 2016: 13) 32
TABLE 4: SELECTED COMPLEXITY METRICS (EXTRACTED FROM COOK AND ZANIN IN COOK AND RIVAS, 2016: 14) 32
TABLE 5: SUMMARY OF FINDINGS FOR RQ1: MAIN INTERNAL AND EXTERNAL DRIVERS OF COMPLEXITY INTO AIR TRAFFIC MANAGEMENT SYSTEM ARCHITECTURE AND (RECIPROCAL) EFFECTS 63
TABLE 6: SUMMARY OF FINDINGS FOR RQ2: SAFETY CULTURE IN THE FACE OF INCREASED SYSTEM COMPLEXITY 64

List of abbreviations

Air Traffic Management Abbreviations:

AIS: Aeronautical Information Service

ANS: Air Navigation Services

ANSP: Air Navigation Service Provider

ATC: Air Traffic Control

ATM: Air Traffic Management

CNS: Communication Navigation Surveillance:

EASA: European Union Aviation Safety Agency

ICAO: International Civil Aviation Organization

MET: Meteorology

SES: Single European Sky

SMS: Safety Management System

System & Complexity Theory Abbreviations:

CNT: Complex Network Theory

CoPs: Complex Products and Systems

CSE: Cognitive Systems Engineering

JCS: Joint Cognitive Systems

LTS: Large Technical Systems

RE: Requirements Engineering

SE: Systems Engineering

STS: Socio-technical Systems