Nonlinear Degradation of System Configuration During the Development of an Accident

Maria Mikela Chatzimichailidou[1,2,*] and Nektarios Karanikas[3]
[1] WSP UK, London, United Kingdom
[2] Imperial College London, United Kingdom
[3] Amsterdam University of Applied Sciences, The Netherlands

ABSTRACT

This paper utilises a methodology named "Risk SituatiOn Awareness Provision" (RiskSOAP). RiskSOAP expresses the capability of a system to meet its safety objectives by controlling its processes and communicating threats and vulnerabilities to increase the situation awareness of its end-users and support their decision-making. In reality safety-related system features might be partially available or unavailable due to design incompleteness or malfunctions. Therefore, respectively, the availability and capability of RiskSOAP mechanisms might fluctuate over time. To examine whether changes in RiskSOAP values correspond to a system degradation, we used the results of a previous study that applied the RiskSOAP methodology to the Überlingen mid-air collision accident. Complementary to the previous application where the RiskSOAP was calculated for four milestones of the specific event, in this study we divided the accident further into seventeen time-points and we calculated the RiskSOAP indicator per time-point. The results confirmed that the degradation of the RiskSOAP capability coincided with the milestones that were closer to the mid-air collision, while the plotting of the RiskSOAP indicator against time showed its nonlinear fluctuation alongside the accident development.

Keywords: Safety; STAMP; STPA; EWaSAP; RiskSOAP.

1. INTRODUCTION

Accident investigation reports show that any degradation in Situation Awareness (SA), such as loss of SA (Salmon et al. 2013), poor SA and lack of SA, may lead to safety issues (BFU 2002; Johnson 2004), especially regarding flight operations (Masys 2005; Salmon, Walker, and Stanton 2015). More specifically, in the analysis of the Überlingen mid-air collision accident, Masys (2005) noted that elements of the socio-technical system, such as the traffic collision avoidance system (TCAS), should not result in the degradation of SA. Moreover, Salmon, Walker, and Stanton (2015) argued that accident investigators need to understand not only what elements of awareness were lost, but what control and coordination transactions between human and non-human agents were either inadequate or required but not present. Thus, risk-focused SA, or simply risk SA, is considered a key factor for systems safety.

Risk SA is defined as the SA of an agent regarding the presence of system-induced or external threats and vulnerabilities that may lead a system to unfavourable states. This SA is facilitated by system features and functions, such as sensors, the maintenance and update of end-users' mental or process models, timely dissemination of safety-related data and information, safety constraints imposed and associated means etc. In this paper, all these are called RiskSOAP mechanisms or elements. If those mechanisms or elements are missing completely or temporarily or they provide the system agents with inadequate services, the capability of the system agents to

* Corresponding author: +44(0)7490276975, mikelachatzimichailidou@gmail.com

fulfil their mission and comprehend the existence of internal and external hazards will erode. The current study is based on the premise that (a) systems carry an inherent RiskSOAP capability, which is directly affected by RiskSOAP mechanisms, and (b) there is a positive association between the RiskSOAP capability and safety.

The RiskSOAP methodology (Chatzimichailidou and Dokas 2015a) is founded on three tools/techniques: (1) the STAMP (Systems-Theoretic Accident Model and Processes) Based Process Analysis (STPA) (Leveson 2011), (2) the Early Warning Sign Analysis based on the STPA (EWaSAP) approach (Dokas, Feehan, and Imran 2013), and (3) a binary dissimilarity measure to depict the distance between the ideal and the real system configurations. The first two tools are used to define the elements and the characteristics that should be included in the "ideal system version". The dissimilarity measure assigns its value to the RiskSOAP indicator. The characterisation of a system version as 'ideal' is used to describe the 'to-be' against its corresponding 'as-is' system version (Chatzimichailidou and Dokas 2015a). The to-be version incorporates preferable additions, alterations or removals of system elements and their corresponding mechanisms and elements based on hazard analysis techniques and early warning sign identification approaches (Leveson 2011, Chapter 2 and Chapter 8). The as-is version of the system is the system as operated. The complete RiskSOAP analysis can be found in Chatzimichailidou, Stanton, and Dokas (2015) and Chatzimichailidou and Dokas (2015a).

In Chatzimichailidou and Dokas (2015a) the RiskSOAP indicator was applied to the Überlingen mid-air collision accident to calculate the distance between the real and the ideal system across four milestones. Based on the published results of Phase 1 and Phase 2 from the analysis of this particular event (Chatzimichailidou and Dokas, 2015b), in the current study the accident timeline was broken down further into seventeen critical points that the authors identified in the official accident investigation reports (BFU 2002; Johnson 2004). More specifically, we used RiskSOAP to measure the distances between the ideal system configuration, as defined by the STPA hazard analysis technique and the EWaSAP approach, and the seventeen actual system versions recorded during the accident progression.

The results allowed the graphical representation of the RiskSOAP values over time with higher detail than the original application of the methodology and revealed the increasing deviation of system configuration from its ideal version as the system was marching towards its total failure.

2. THE ÜBERLINGEN MID-AIR COLLISION

The airspace where the two aircraft were operating and approaching each other was controlled by the Zurich services. Normally, two Air Traffic Controllers (ATCs) handle the airspace, however, due to rare arrival traffic that night, one controller was on a break, and the other was monitoring two displays located a meter apart. Maintenance of the main radar system was in progress overnight, and the radar was in fall-back mode, meaning that it provided only aural STCA warnings. The lack of a visual warning system corresponded to a lower potential of the system to inform timely and effectively the ATC. On the night of the accident, the main telephone system that enables ATCs to communicate with each other was out of service due to maintenance, and the backup system had a software failure. Under these circumstances, the single ATC on duty could not timely realise the problem of the imminent aircraft collision.

Only less than a minute before the accident did the ATC of the Swiss airspace control service realised the danger and contacted Flight 2937 and instructed them to descend to avoid the collision. The TCAS on Flight 2937 instructed the pilots to climb, and the TCAS on Flight 611 to descend. Flight 611 initially followed the TCAS instructions and initiated a descent, but they could not immediately inform the ATC because the controller was dealing with the other flight. Flight 2937 disregarded the TCAS instruction to climb and began to descend as instructed by the ATC. Therefore, both aircraft were descending simultaneously. Unaware of the TCAS-issued alerts, the ATC repeated his instruction to Flight 2937 to descend, giving Flight 2937 incorrect information about the position of Flight 611 (Nunes and Laursen 2004). Figure 1 offers an overview of the accident development. It starts from the first milestone at which "both ATCs report for duty" [Time:

17:50:XX], goes through all the 15 intermediate milestones, until the seventeenth and final milestone at which the "TCAS instruction 'increase climb' to TU154M (i.e. Flight 2937) is commented only by the co-pilot, but he does not find audience" [Time: 21:35:24].

The timeline consists of 17 important milestones where the state of important system features impacting safety differed from their previous state. In the Figure presented in the Appendix, the first and the last milestones were omitted for the better clarity of the figure. Due to space-saving reasons, some events are not included in the particular Figure. The additional events at the different milestones are as follows:

Milestones	Eventuality
7	ATC works from 2 adjacent workstations, with 3 different functions, performs radio communications on 2 frequencies
	ATC tries to call Friedrichshafen without success (defect in the by-pass phone system)
8	B757 co-pilot does not notice conflicting traffic on the VSI/TRA
11	Disagreement between the TU154M crew members because of ATC≠TCAS instructions
	ATC instruction to TU154M to descent not yet verbally acknowledged
16	TU154M do not react to the B757 report about TCAS descent
	ATC does not hear the B757 message (TCAS descend)

3. METHODOLOGY

In the analysis performed by Chatzimichailidou and Dokas (2015b), STPA and EWaSAP had generated a total of 278 specifications, formulated as requirements. The presence of each requirement was assigned the number "1" whereas each absence was assigned the number "0". Through the assignment of values, it was possible to translate linguistic representations into numerical ones. Hence, using the ideal system vector as the point of reference, the values of the real system vector were obtained by mapping the present and absent system elements in the seventeen real system vectors. Afterwards, the Rogers-Tanimoto dissimilarity value (Choi, Cha, and Tappert 2010) was calculated for all seventeen vectors (Figure 1) as well as the differences between these values from their preceding ones. It is noticed that the dissimilarity values can range from "0" to "1", where "0" denotes that the system is ideally configured and "1" means that the system lacks all elements necessary to meet its safety objectives.

To evaluate the results qualitatively, we plotted the RiskSOAP values against the corresponding accident milestones and the timeline of the accident. Based on the distribution of data points revealed on the graph, as presented in the following section of the paper, we processed the data with SPSS version 22 (IBM 2013) and examined their fit to the Quadratic and Qubic regression models. Due to the large time gap amongst the first accident milestones, curve estimation calculations were possible only from Milestone 8 and later.

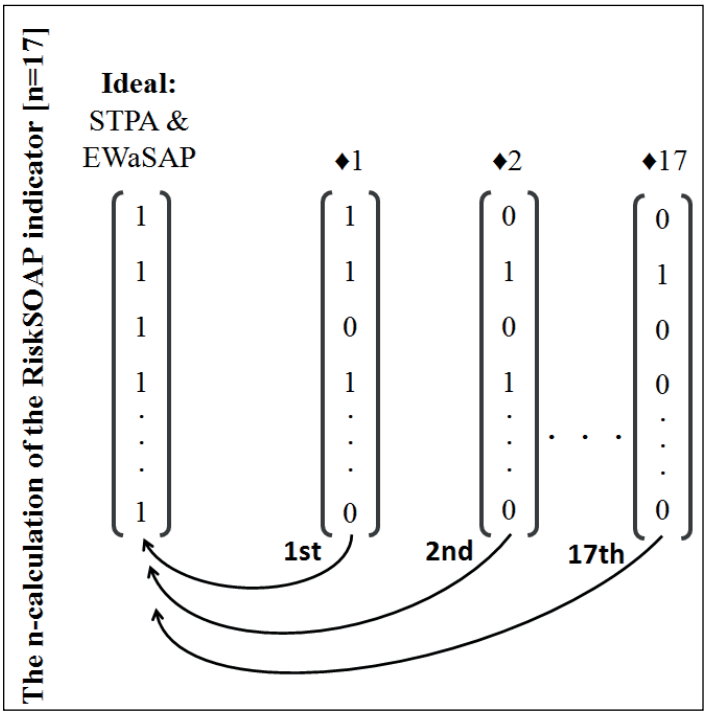

Figure 1: Examples of vectors used to calculate the Rogers-Tanimoto measure

4.RESULTS

The numerical results of the RiskSOAP values and the differences between their adjacent values are presented in Table1, where the number of system elements and safety constraints that are present in the real system gradually decreases along the development of the accident. Milestone 3 is the only one where the number of present elements increases compared to its preceding time-point. Namely, at Milestone 2, the departing supervisor did not inform the ATC about the impact of Sectorisation. However, at Milestone 3 the ATC himself realised the degradation in the available services when his workstation was switched to fall-back mode. Therefore, the ATC makes up for the lack of briefing by using and combining other sources of information.

The values responding to the “RiskSOAP indicator” column of Table 1 reveal that a ‘worsening’, i.e. ‘↑’, evolves in parallel with the accident development. When a technical (e.g. “direct telephone lines to the neighbour ATC units are not available”, Milestone 5) or a human (e.g. “2nd ATC assistant retires to rest”, Milestone 6) agent degrades, the RiskSOAP indicator increases and indicates a larger distance from the ideal system; the gradual increase of the RiskSOAP value signifies the deterioration of the RiskSOAP capability. The last column of Table 1, i.e. “Difference”, lists the values that convey the change of the RiskSOAP indicator from milestone to milestone. As stated previously, there is only one point where a ‘betterment’ between Milestone 2 and Milestone 3 is observed.

Table 1 The RiskSOAP values against the accident milestones

Milestones	Present	Absent	RiskSOAP indicator	Difference
♦1	179	99	0.5252	-
♦2	166	112	0.5744↑	0.0492

Milestones	Present	Absent	RiskSOAP indicator	Difference
♦3	170	108	0.5596↓	-0.0148
♦4	168	110	0.5670↑	0.0074
♦5	166	112	0.5744↑	0.0073
♦6	166	112	0.5744-	0.0000
♦7	158	120	0.6030↑	0.0287
♦8	152	126	0.6238↑	0.0207
♦9	149	129	0.6339↑	0.0101
♦10	144	134	0.6505↑	0.0166
♦11	132	146	0.6887↑	0.0382
♦12	127	151	0.7040↑	0.0153
♦13	127	151	0.7040-	0.0000
♦14	125	153	0.7100↑	0.0060
♦15	120	158	0.7248↑	0.0148
♦16	119	159	0.7277↑	0.0029
♦17	118	160	0.7306↑	0.0029

The left chart of Figure 2 shows the increase in the RiskSOAP indicator value, representing the degradation of the RiskSOAP capability from the first until the seventeenth milestone, without any time reference. On the right chart of Figure 2, the calculated difference between the values of two successive RiskSOAP indicator measurements is given. Both charts correspond to the values of the two last columns of Table 1.

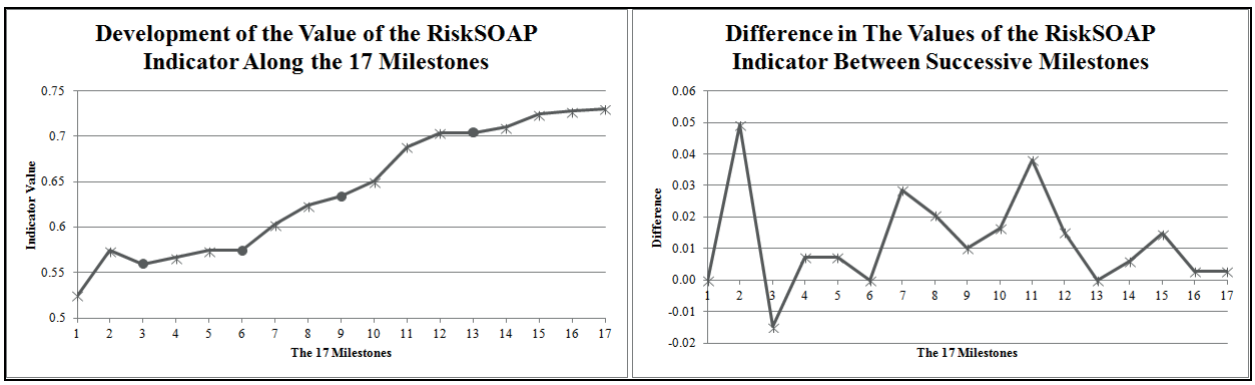

Figure 2: The values of the RiskSOAP indicator along the 17 milestones of the Überlingen accident (left chart) and the difference between successive measurements of the RiskSOAP indicator (right chart)

Figure 3 depicts the change of the RiskSOAP indicator along the Überlingen accident timeline. Each dot on the diagram represents one of the 17 milestones of the accident. The first milestone is reached around 17:50. The first value of the RiskSOAP indicator is 0.5252, as shown in Table 1, and indicates that the night of the accident the system configuration was already far from optimal. The last dot at 21:35:24 hrs and the RiskSOAP value 0.7306 correspond to the 17th and last milestone where the co-pilot of the TU154M was able to comprehend the situation, but due to the lack of sufficient RiskSOAP capability on a system level his “warning” message was omitted.

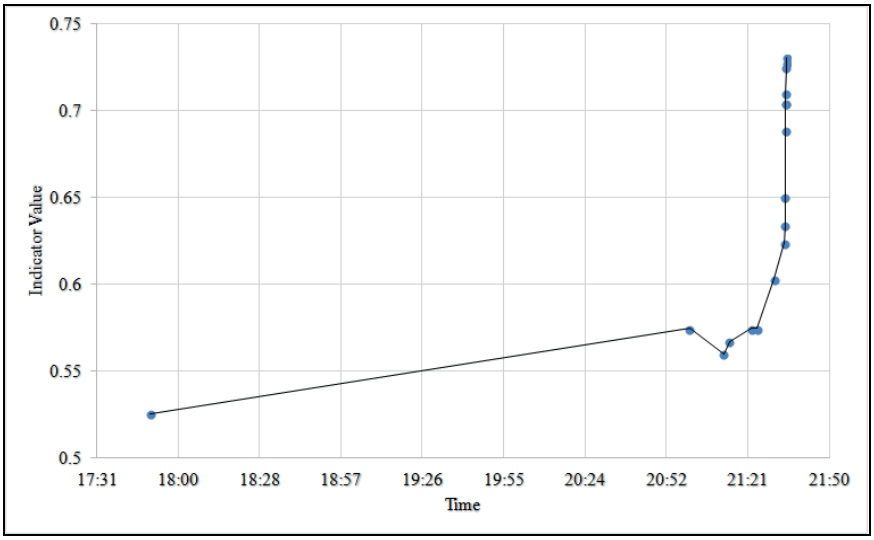

Figure 3: The RiskSOAP indicator values along the Überlingen accident timeline

The curve estimations from Milestone 8 until Milestone 17 generated the plots presented in Figures 4 for the Quadradic model and Figure 5 for the Cubic curve. The results from SPSS indicated a better fit of the data to the Cubic regression model as indicated by the R^2 values (Quadradic: R^2=0.925, p=0.000; Cubic: R^2=0.971, p=0.000). The detailed parameter estimates are not reported because the goal of the study was to examine the (non)linear progression of the RiskSOAP values and not to suggest any specific model fit that could be considered for any event; every accident regards a different system within a given context and carries unique characteristics.

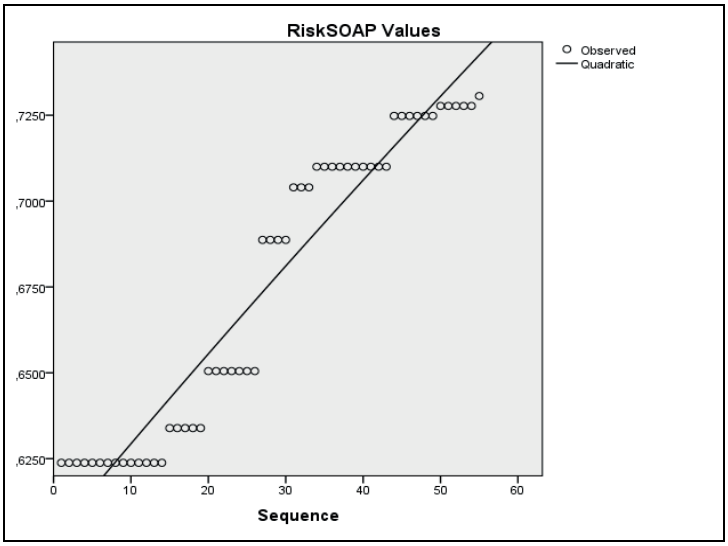

Figure 4: The RiskSOAP values against the Quadratic regression curve

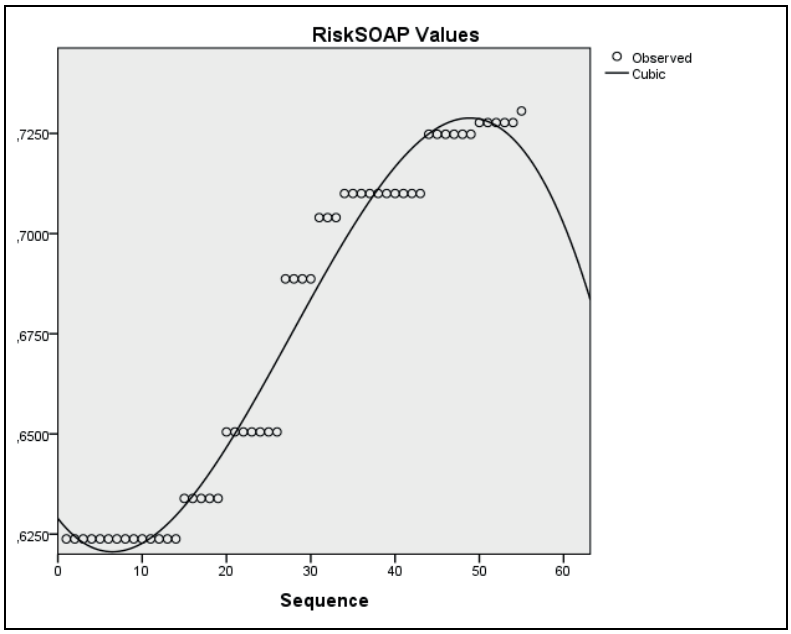

Figure 5: The RiskSOAP values against the Cubic regression curve

5.DISCUSSION

Overall, the left diagram of Figure 2 shows a continuous decrease of the RiskSOAP capability as the event advances, and Figure 3 reveals a non-linear behaviour of the RiskSOAP indicator. The latter is also seen in Figures 4 and 5, which correspond to non-linear regression models. Furthermore, the fluctuations of the values, which are clearer on the right chart of Figure 2, confirm the lack of linearity of the changes in the RiskSOAP capability. Practically, the findings provide support to the argument that socio-technical systems exhibit non-linear behaviours and drift into failure incrementally (Dekker 2012). The accident occurred just a few seconds after the RiskSOAP indicator reached its maximum value calculated (i.e. 0.7306) indicating that it is not necessary to violate every safety constraint and miss all system elements to lead a system to its catastrophe. However, each system has a different set and functionality of reinforcing and feedback loops and is not expected to drift into a failure irrecoverably at the same RiskSOAP values.

Interestingly, there is one time-point with a decreasing indicator value (i.e. Milestone 3), which corresponds to the case where one system element may compensate for the degradation of the RiskSOAP capability caused by the loss or misbehaviour of another system element. Moreover, both minor and major differences between two successive values of the indicator are observed. An example of a minor difference is the one between Milestone 8 and Milestone 9 (Figure 2-right chart and Table 1). On the other hand, the difference between Milestone 10 and Milestone 11 (Figure 2-right chart and Table 1) is a larger one. Also, most of the losses regarding the available system elements were observed and recorded at Milestones 2, 7, 11, and 15, (i.e. peak values in Figure 2-right chart) that had unequal time differences from one another. The authors would like to note that, as Salmon, Walker, and Stanton (2015) explained, the loss of Situational Awareness in this paper has a broader meaning and regards the system as a whole; not its elements alone. To render a system aware of its state and external threats, its overall configuration, as measured by the RiskSOAP, must support effective control of processes and feedback information. As stated in the introduction section above, it is important to investigate not only what sort of awareness was lost, but also what transactions between the system elements were either inadequate or required but not forthcoming (Salmon, Walker, and Stanton 2015). This is the reason why RiskSOAP is not applied only to the system sensors and feedback mechanisms,

but analyses the whole set of components and requirements needed to allow the system to meet its objectives.

6.CONCLUSION

This work extends the study of Chatzimihailidou and Dokas (2015b), which had initially indicated that in the Überlingen accident the degradation of the RiskSOAP capability was happening gradually and in parallel with the degradation or loss of technical and human services, and information. At the same time, according to the BFU (2002) official accident investigation report, the deterioration or loss of those system elements and their characteristics caused a safety drift that finally led to the accident.

The main contribution of the current paper is that, to the best of our knowledge, this is the first work that provides a numerical and graphical visualisation of how the capability of a system to accomplish its mission successfully deteriorates in a nonlinear manner as the system migrates to a state of loss as reflected by the gaps between its ideal and current configurations. These gaps, which were measured with the RiskSOAP indicator at seventeen milestones of the Überlingen accident, can be attributed to the absence or malfunction of system elements, inadequate interactions, inherent design flaws and unsafe control actions. All these conditions allow a system to slip into unfavourable states that cannot be predicted with linear methods and are specific to the configuration and dynamic behaviour of the system.

On the downside, the numerical figures calculated in this work cannot be generalised. A single case study is not adequate enough to suggest RiskSOAP values after which every system might drift into severe events irrecoverably or, in other words, what the maximum RiskSOAP value is before which a system has still the opportunity to recover and avoid a catastrophe. Further studies of similarly complex systems are required to provide possible indications of the size of the gaps between ideal and real system configurations that can affect system performance negatively and dramatically. Nonetheless, the authors plan to apply the COSYCO indicator (Karanikas and Chatzimichailidou 2018) to the same and other case studies. COSYCO compensates for the limitations detected for the RiskSOAP indicator (Chatzimichailidou and Dokas 2015a) and evaluates the fluctuation of the differences between system states by considering (1) the system level each requirement is (partially) met or not, and (2) the dependencies of each element on other system components.

REFERENCES

Chatzimichailidou, M. M., & Dokas, I. M. (2015a). Introducing RiskSOAP to communicate the distributed situation awareness of a system about safety issues: an application to a robotic system. *Ergonomics*, *59*(3), 409-422.

Chatzimichailidou, M. M., & Dokas, I. M. (2015b). The Risk Situation Awareness Provision Capability and its degradation in the Überlingen accident over time. *Procedia Engineering*, *128*, 44-53.

Chatzimichailidou, M. M., Stanton, N. A., & Dokas, I. M. (2015). The concept of risk situation awareness provision: towards a new approach for assessing the DSA about the threats and vulnerabilities of complex socio-technical systems. *Safety science*, *79*, 126-138.

Choi, S. S., Cha, S. H., & Tappert, C. C. (2010). A survey of binary similarity and distance measures. *Journal of Systemics, Cybernetics and Informatics*, *8*(1), 43-48.

Dekker, S. (2012). *Drift into failure: From hunting broken components to understanding complex systems*. CRC Press.

Dokas, I. M., Feehan, J., & Imran, S. (2013). EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. *Safety science*, *58*, 11-26.

German Federal Bureau of Aircraft Accident Investigation - Bundesstelle für Flugunfalluntersuchung. (2004). *BFU Überlingen Investigation Report.* Reference AX001-1-2/02.

IBM. (2013) SPSS Statistics for Windows. Version 22.0. New York: IBM Corp.

Karanikas, N., & Mikela Chatzimichailidou, M. (2018). The COSYCO Concept: an Indicator for COmparing SYstem COnfigurations. *AUP Advances*, *1*(1), 154-174.

Johnson, C. W. (2004). Final report: review of the BFU Überlingen accident report. *Contract C/1.369/HQ/SS/04. Eurocontrol*.

Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT press.

Masys, A. J. (2005). A systemic perspective of situation awareness: An analysis of the 2002 mid-air collision over ÜBerlingen, Germany. *Disaster Prevention and Management: An International Journal*, *14*(4), 548-557.

Nunes, A., & Laursen, T. (2004, September). Identifying the factors that contributed to the Überlingen Midair Collision. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 48, No. 1, pp. 195-198). Sage CA: Los Angeles, CA: SAGE Publications.

Salmon, P. M., Beanland, V., Lenné, M. G., Filtness, A. J., & Stanton, N. A. (2013). Waiting for Warning. In *Contemporary Ergonomics and Human Factors 2013* (Vol. 403, No. 410, pp. 403-410). ROUTLEDGE in association with GSE Research.

APPENDIX

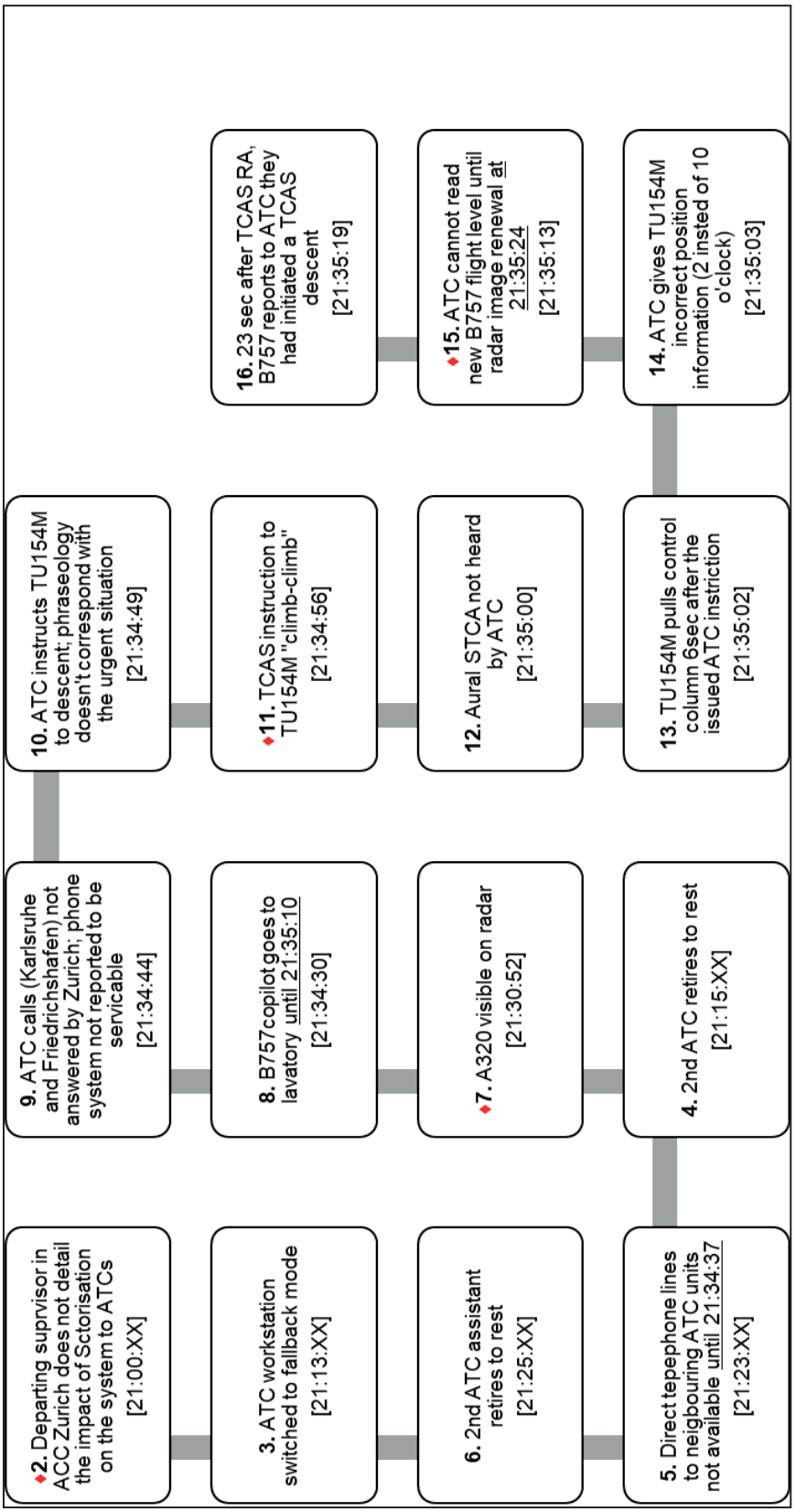

Figure A.1: The seventeen milestones