Assessing Distributed Situation Awareness in Socio-Technical Systems with RiskSOAP

Maria Mikela Chatzimichailidou(✉) and Ioannis M. Dokas

Department of Civil Engineering, Democritus University of Thrace, Vassilissis Sofias 12, 67100 Xanthi, Greece
{mikechat, idokas}@civil.duth.gr

Abstract. This research work introduces the Risk Situation Awareness Provision (RiskSOAP) methodology. The concept of 'risk SA provision' reflects the inherent, according to the system design and development, capability of each system part to provide its agent with SA about the presence of system threats and vulnerabilities, possibly leading to accidents. The RiskSOAP methodology is accompanied by its corresponding indicator, which is used to measure the capability of a complex socio-technical system to provide its agents with Situation Awareness (SA) about the presence of its threats and vulnerabilities. The RiskSOAP indicator also enables analysts to assess Distributed SA (DSA). RiskSOAP is applied to the socio-technical system involved in the Überlingen mid-air collision accident as a demonstration of how to apply the methodology and calculate the corresponding indicator.

Keywords: Dissimilarity measures · Distributed situation awareness · EWaSAP · Safety · STPA · RiskSOAP

1 Introduction

In the literature there is a plethora of definitions for SA. One widely cited definition proposes SA as a state of working knowledge of an individual; it is how much and how accurately he/she is aware of the current situation and concerns (1) the perception of the elements within a system, (2) the comprehension of their meaning, and (3) the projection of their future state [1] The number of proposed definitions is analogous to the models which explain the different types of SA, including: the individual SA model [1], the team and shared SA models [2, 3], the meta [4], compatible [3], and collective [5] SA models, and the most complex one, the DSA model [6]. DSA implies that no one system agent, namely humans and automated controllers within a system has a complete picture of the situation in which the system finds itself, but just a facet of the corresponding situation at any point in time [4].

So far, the only reported DSA-focused method is the Event Analysis of Systemic Teamwork (EAST) [7]. It makes use of three networks, i.e. task, social, and information ones, that describe the relationships between tasks, their sequence and interdependencies, the organisation of the system and the communications between agents, along with the information that these agents use and communicate [7]. However, EAST is not a DSA measurement technique, but finally offers a depiction of information flow

N. Bellamine Ben Saoud et al. (Eds.): ISCRAM-med 2015, LNBIP 233, pp. 103–115, 2015.
DOI: 10.1007/978-3-319-24399-3_9

between the interacting human and nonhuman agents [8]. It is a stepwise description and guidance for studying and depicting agents and networks of agents involved in the acquisition and maintenance of DSA through information processing and assessment. The outcome of this method is qualitative and it mostly bears a resemblance to semantic networks [8].

The RiskSOAP methodology embraces a different perspective, compared to any other SA measurement technique that carries at least one of the *Seven Issues on DSA* [8], as recorded in the literature. According to those seven issues, complex socio-technical systems require more holistic reasoning and targeted approaches that the existing ones that focus either on individuals or on teams of individuals [8]. Overall, compared to RiskSOAP, no other, reported so far, SA measurement technique, gives a quantitative expression to the risk SA provision capability (for more see [8, 9]).

Turning to the subject of '*risk SA provision*', it reflects the inherent, according to the system design and development, capability of each system part to provide its agent with SA about the presence of system threats and vulnerabilities, possibly leading to accidents. In short, this capability stems from the number, type, and characteristics of each one of the system elements that together shape the different parts of it, laying thus the foundation for the emergence of risk DSA [9]. As a result, all or some parts of a socio-technical system can be designed and developed with more or less enhanced risk SA provision capabilities, integrating or leaving out elements, such as sensors capable of detecting more threats and vulnerabilities as well as agents whose mental or process models sufficiently represent possible accident scenarios etc.

The RiskSOAP methodology is applied to the Überlingen mid-air collision accident in order to demonstrate how to take the steps of the methodology and finally calculate the value of the corresponding indicator as an assessment of the system's DSA. Using the Überlingen accident, this paper also provides evidence that the risk SA provision capability is dynamic by nature in a manner that it varies according to the design specifications of each complex socio-technical system [9].

However, the main contribution of this paper is not the use case, but the RiskSOAP methodology for assessing DSA regarding safety issues. Given that systems consist of specifications and components possible to be mapped, RiskSOAP demonstrates the feasibility of measuring to what extent systems' elements contribute to the emergence of DSA.

2 The RiskSOAP Methodology

The methodology is grounded on two pivotal assumptions:

Assumption 1. The awareness of threats and vulnerabilities (i.e. the risk SA) enhances safety. This assumption accords to the works of [10, 11] supporting the positive correlation between safety and awareness.

Assumption 2. An 'ideal', in terms of the risk SA provision capability and risk DSA, system design could derive from hazard analyses, because they help designers gather essential system elements and characteristics that ideally should be included into the system design, serving to enhance its preparedness against accidents.

Grounded on these two assumptions, the methodology goes through three stages: (1) in terms of the system perceiving its threats and vulnerabilities, define the 'ideal'[1] or otherwise the 'to-be' image[2] of the system using a comprehensive hazard analysis and early warning sign identification techniques, (2) identify the real or otherwise the 'as-is' one, (3) employ a comparative strategy aiming to depict the distance between the two images of the system and interpret the distance value, obtained by the introduced indicator, on the basis of risk DSA. The phases of the RiskSOAP methodology are presented in Table 1.

Table 1. The RiskSOAP phases and steps.

Phase 1↓	Step 1.1. perform the STPA hazard analysis Step 1.2: carry out the EWaSAP approach
Phase 2↓	Step 2.1: create the ideal system vector Step 2.2: create the real system vector
Phase 3	Step 3: apply Rogers-Tanimoto dissimilarity measure

Existing approaches (from unrelated to each other research fields) are utilized to fulfill the objectives of the 1st and the 3rd Phase of the methodology. The methods used by RiskSOAP are: (1) the STAMP Based Process Analysis (STPA) [12] and (2) the Early Warning Sign Analysis based on the STPA (EWaSAP) approach [13], which both define the elements and the characteristics that should be included in the ideal image of the system, and (3) a binary dissimilarity measure to depict the distance between the ideal and the real system image.

Nevertheless, the researcher can use any other hazard analysis, early warning sign identification approach, or dissimilarity/similarity measure he/she prefers.

2.1 STPA and EWaSAP

Leveson's Systems-Theoretic Accident Model and Processes (STAMP) [12] advocates that accidents involve a complex, dynamic process, meaning that they are not simply chains of component failure events. Safety is treated as a dynamic control problem, rather than a component reliability problem. It is also an emergent property that arises when system components interact with each other within a larger environment. While encapsulating the STAMP principles, STPA is a top-down hazard analysis technique that generates high-level safety requirements and constraints. Compared to traditional hazard analysis techniques, e.g. fault and event tree analyses, STPA identifies not only detectable events, such as technical failures or human errors, but also inadequate control actions and scenarios or paths to accidents. It does not generate a probability

[1] No methodology can perfectly fit all purposes or cover all aspects of a complex socio-technical system. However, an approximation of its behaviour and components can be based on systems theoretic hazard analysis techniques and early warning sign identification approaches.

[2] The word 'image' was intentionally chosen, since the methodology is inspired by pattern matching; a comparison between a target image template and a query image.

number related to a hazard, since the only way to generate such a probability of an accident for complex systems is to omit important causal factors that are not stochastic or for which probabilistic information does not exist [12].

EWaSAP extents STPA by adding extra steps to guide analysts in identifying those perceivable signs, which indicate the presence of flaws and the violations of designing assumptions during the operations phase of a system [13]. EWaSAP introduces an additional type of control action, the awareness action. An awareness control action allows a controller to provide warning messages and alerts to other controllers inside or outside the system boundaries, whenever data indicating the presence of threats or vulnerabilities is perceived and comprehended. Table 2 shows the sequence of executing the STPA and the EWaSAP steps as one process.

2.2 Dissimilarity Measures

In the literature, there are plenty of distance/dissimilarity measures, which detect the mismatching bits of two binary data sets. The selection of the proper dissimilarity measure is customised to the assumptions made by the investigator during a specific problem statement. In this paper, Rogers-Tanimoto is chosen, on the basis that it is the only Boolean metric that gives weight to the dissimilarities between two compared vectors by multiplying them by two, i.e. '2*S10', '2*S01'. Its formula is [14]:

$$RTd(i,r) = \frac{2S10 + 2S01}{S11 + S00 + 2S10 + 2S01} \quad (1)$$

The terms: 'S00', 'S01', 'S10', 'S11' denote the total number of the corresponding (0,0), (0,1), (1,0), and (1,1) pairs of binary integers, of the two compared vectors. Figure 1 conveys that in order for vectors to be compared they have to have the same number of rows; the number of rows for both vectors on Fig. 1 is 5. There is therefore a one-by-one relationship between the binary integers that shape a specific pair.

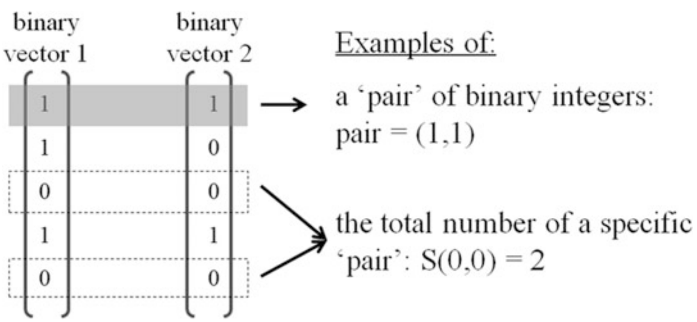

Fig. 1. A graphical explanation of the 'pairs' and 'totals' for the dissimilarity measures.

Table 2. The STPA and EWaSAP steps.

STPA steps and description	EWaSAP steps and description
STPA(1): Identify system hazards & translate them into top-level safety constraints	
	EW(1): Decide if there is anyone outside the system who needs to be informed about the perceived progress of the hazard or about its occurrence
STPA(2a): Create control structure	
STPA(2b): For each controller in the control structure identify its unsafe control actions	
STPA(2c): Restate the inadequate control actions as safety constraints/requirements	
	EW(2): Aim: Identify useful sensory services (i.e. video surveillance cameras pointing) installed in or possessed by systems outside of the system in focus and establish synergy
	EW(2a): For each top level safety constraint identify those signs which indicate its violation
	EW(2b): Find those systems in the surrounding environment with sensors capable of perceiving the signs defined in EW(2a) & request to establish synergy
STPA(3a): For each controller in the control structure create a model of the process it controls	
STPA(3b): Examine the parts of the control loops to determine if they can contribute to or cause system level hazards	
	EW(3): Aim: Enforce Internal Awareness Actions
	EW(3a): Describe what needs to be monitored & what type of features/capabilities the sensors must have so that to make the appropriate controllers capable of perceiving: - the signs indicating the occurrence of the flaw - the violation of the assumptions made during the design of the system
	EW(3b): After design trade-offs and selection of sensors, define which patterns of perceived data indicate the occurrence

(*Continued*)

Table 2. (*Continued*)

STPA steps and description	EWaSAP steps and description
	of the flaw and/or the violation of its designing assumptions
	EW(3c): Update the process models of the controllers with appropriate awareness and control actions, which should be enforced based on the perceived early warning signs, so that to warn about, adapt to, or eliminate the causal factor to the loss which is present in the system
	EW(3d): For each perceived warning sign, define its meta-data/attribute values to ensure that it will be perceived and ultimately understood by the appropriate controller/s
STPA(4): Restate any flaws identified as safety constraints & repeat STPA(3a) & STPA(3b)	

Some facts about dissimilarity measures are the following: (a) The minimum dissimilarity is ‘0’; when the dissimilarity of two binary vectors tends to ‘1’, then the vectors are almost dissimilar. (b) All variables are brought into a common scale, between ‘0’ and ‘1’, i.e. they are normalised. (c) Distance can be defined as a dual of a similarity measure d(i,r) = 1 - s(i,r); a similarity can be expressed as the complementary of the corresponding dissimilarity, and vice versa.

3 The Überlingen Mid-Air Collision Accident

In this accident two aircraft (i.e. Flight 2937 and Flight 611) controlled from Zurich were on a collision course. Normally, two ATCs handle the airspace, but because of low arrival traffic at the airport that night, the one of them was on a break and the other was monitoring simultaneously two display consoles, separated by over a meter. The main radar system was functioning in fallback mode overnight, without visual but with aural Short Term Conflict Alert (STCA) warning system, meaning that the ATC had to use a slower system. Additionally, on the night of the accident the main telephone system that enables ATCs to communicate with one another was out for maintenance and the back-up system had a software failure, which no one in the company had noticed. Under these circumstances, the only ATC on duty did not realise the problem in time, and thus failed to keep the two aircraft at a safe distance from each other [15]. Only less than a minute before the accident did the ATC realise the danger and contacted Flight 2937, instructing the pilots to descend in order to avoid the collision. The TCAS on Flight 2937 instructed the pilots to climb, and the TCAS on Flight 611 instructed the pilots to descend. Flight 611 initially followed the TCAS advisory and initiated a descent, but they could not immediately inform the ATC, due to the fact that he was dealing with Flight 2937. However, Flight 2937 disregarded the TCAS advisory to climb, and instead began to descend, as instructed by the ATC, thus both airplanes were now descending. Unaware of the TCAS-issued alerts, the ATC repeated his instruction to Flight 2937 to descend, giving the crews incorrect information as to their relative position.

As regards the causes of the accident, official accident reports [16, 17] involve both (a) technical and (b) organisational deficiencies. Referring to the technical ones, the German Federal Bureau of Aircraft Accident Investigation (BFU) [16] puts emphasis on the operation of the radar system in fallback mode. This degradation of the radar services induced more “system degradations” and “unusual situations” [16]: (1) no automatic correlation of the flight targets was possible and the optical STCA was not displayed, (b) the direct phone connections with the adjacent ATC units were not available to the ATC in Zurich, thus the calls from adjacent ATCs were registered but not answered. Besides, the written directives concerning the accomplishment of the work did not include explanations about the effects that the fallback mode would have on the availability of technical equipment [16]. With reference to the TCAS, BFU [16] argues that it normally contributes to the awareness of the crew, however, in the case of Überlingen it finally contributed to the accident because the regulations concerning TCAS were not standardised, but incomplete and partially contradictory. Finally, due to no automatic TCAS downlink in place, carrying information about the issued advisories to the ATCs, radio delays and loss of information were possible to occur [18]. Referring to organisational issues, in the BFU [16, p.84] accident investigation report is stated that: “at the conscious level humans have limited attention resources. When these limited resources are time-shared between multiple demanding tasks, as in the case of the controller, the continuous detailed analysis of all incoming external information is not possible”. This practically means that the single man operation deteriorated the ATC’s workload and reduced his ability to maintain an awareness of the situation in a timely manner. Under the same notion, Wong [18] regards information sharing among team members as a variable that positively affects controller’s SA. Referring again to the ATC, Johnson [17, p.9] points out that “it is difficult to determine what might have made him aware of the potential conflict…it seems much more of a coincidence that the controller responded”. This gives rise to the implication that there was no official mechanism for making the ATC aware of the situation in the airspace.

4 Applying RiskSOAP to the Überlingen Accident

As illustrated in Table 1, the RiskSOAP methodology consists of three phases. In Phase 1 and while considering that there are no limitations regarding the available resources, the STPA hazard analysis (Step 1.1) establishes safety constraints/requirements to define the ideal image of the system. Similarly, internal sensory services to capture early warning signs are determined by the EWaSAP approach in Step 1.2.

Based on the above findings, in Phase 2 one can create the ideal system vector (Step 2.1) consisting of qualitative values, i.e. safety requirements and sensory services.

Similarity, the real system vector is built (Step 2.2) by tabulating all elements that exist in the real system, as it is designed, and those that, according to Phase 1, should ideally be incorporated into the design, but they may be either present or absent. Then, all elements of both vectors have to be translated into quantitative ones, i.e. take binary values. These two vectors are the input to the dissimilarity measure.

In Phase 3, Step 3, Rogers-Tanimoto (Eq. 1) is chosen as a dissimilarity measure for comparing the two vectors. Thus, the 'S00', 'S01', 'S10', and 'S11' terms on Eq. 1 have to be substituted so as to calculate the value of the indicator. The obtained value express the inherent capability of the system to provide its agents with risk SA provision. Relying on the measurement of this capability, one can determine the degree to which system's risk DSA can be further enhanced.

4.1 Results

In this example, STPA was applied first, followed by EWaSAP. Beginning with the steps of the STPA hazard analysis, in STPA (1) the accident/losses, hazard(s), and system level safety constraints were defined:

Accident/losses definition: Loss of human life due to aircraft collision

Hazard: A pair of controlled aircraft violate minimum separation standards

System level safety constraint: The ATC must provide: (a) advisories that maintain safe separation between aircraft and (b) conflict alerts

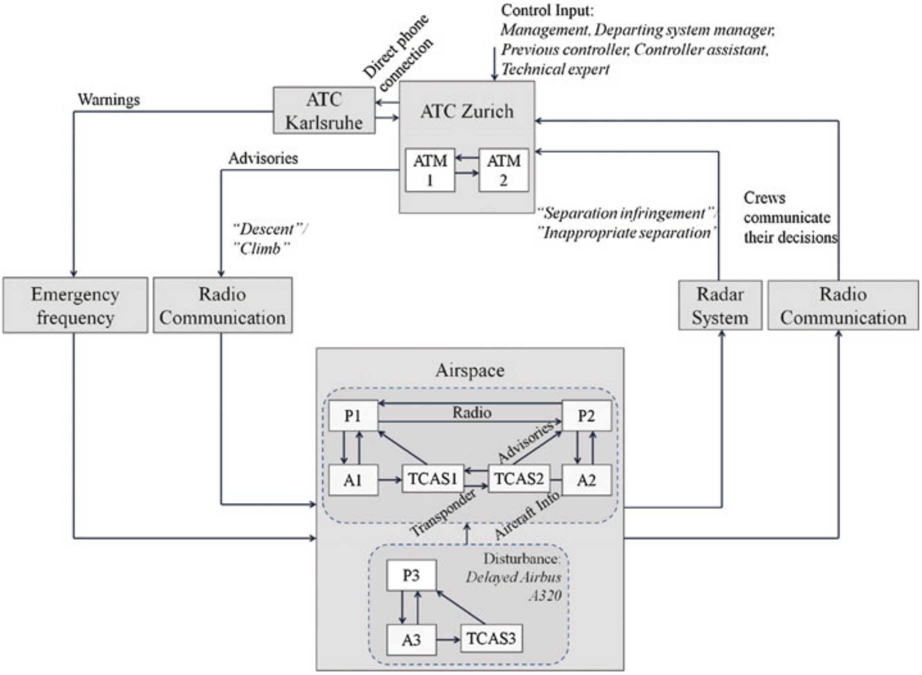

Fig. 2. The control structure of the systems involved in the Überlingen accident.

Table 3. Indicative results from the first phase of the RiskSOAP methodology.

System elements	STPA & EWaSAP	Original system
Safety requirements		
ATC Zurich		
1. When STCA is working in fallback mode the acoustical warning should be switched on at the beginning of the night shift	1	1
ATC Karlsruhe		
2. The Bypass System should be always available to the ATC, or in cases where it is out of service the ATC should be informed	1	0
Crews		
3. Time to comply with new safety policy requirements should be given to the officers	1	0
TCAS		
4. There should be a downlink in place to pass the TCAS advisories to the ATC	1	0
Sensor characteristics		
ATC Zurich		
5. Should be aware whether the radar system is working in fallback mode	1	1
ATC Karlsruhe		
6. Should be aware how long the Bypass System is out of order	1	0
Crews		
7. Should read the training hours of the pilots in unique situations	1	1
TCAS		
8. Should see the position of the TCAS/which modes are available	1	1
Mental models and Control algorithms		
ATC Zurich		
9. If "horizontal separation (from radar returns) ≤ 5 NM (≈ 9 km)" OR "vertical separation ≤ 1000 ft (≈ 300 metres)" Then "separate converging components: climb/descent to z FL (i.e. Flight Level)"	1	1
ATC Karlsruhe		
10. If "altered by his STCA of conflict situation" Then "warn the adjacent ATC by phone" If "warning not received by the adjacent ATC" Then "try again" Else "select international emergency frequency to contact crews"	1	0

In STPA(2a) the safety control structure of the Überlingen case was created, as depicted in Fig. 2.

ATC Zurich is the main controller of the two, directly involved in the accident, aircraft. He also communicates, and in case of emergency is aided by, with an adjacent but external controller; the ATC Karlsruhe. The former issues commands to the aircraft (here, three aircraft are controlled) via radio communications (see Fig. 2, left side). Again, in case of emergency, the latter can use international frequencies to reach the crews, although they are not under his control. Data from what is happening within the airspace controlled by the ATC Zurich is passed to him through the radio and radar system (see Fig. 2, right side).

The total number of safety requirements and sensor characteristics was 279; 119 safety requirements and 152 sensor characteristics were obtained by taking the STPA and EWaSAP steps respectively. Furthermore, 8 mental models and control algorithms were the output of the combination of the responsibilities and the safety constraints that each of the controllers of the system involved in the Überlingen accident should possess. Some indicative results are given in Table 3.

Every component of the 279-sized vector that came up from STPA and EWaSAP was equal to ‘1’ because it reflected the ideal system design version. For the original design version, as it was involved in the accident, the elements detected by STPA and EWaSAP being absent from the systems were assigned the value ‘0’, while the rest of them were given the value ‘1’.

Given the above binary values (along with those not included in the paper in hand due to space limitations), the Rogers-Tanimoto dissimilarity measure was calculated. The precise values are given in Table 4.

Table 4. Overall numerical results for the Überlingen accident.

System elements	STPA & EWaSAP (ideal)	Original system (real)
present:	279	74
Absent:	–	205
Vectors’ length:	279	279
RiskSOAP indicator: RTd(i,r)=		=2*205 + 2*0/74 + 0 + 2*205 +2*0 =0.8471

As depicted in Table 4, from the 279 system elements identified by STPA and EWaSAP, the number of present system elements in the original system were 74; 205 were the absent ones. The number of 279 total system elements signify the length of the two combined vectors.

The RiskSOAP indicator value obtained after comparing the ideal system vector to the original one was 0.8471. This value is the measurement of the risk SA provision capability and constitutes an assessment of DSA for the Überlingen case. As an example, the value derived from the RiskSOAP indicator implies that the ATC Zurich may not to be able to perceive and prevent a hazard identified by STPA. If one recalls the conditions under which the Überlingen accident occurred, due to the STCA working in fallback mode, the ATC Zurich was not able to comprehend the two aircraft being in collision trajectory, at least not in time. This restricted operation of the STCA system (among others) is implied by the calculated RiskSOAP value. If the STCA working in fallback mode is to be remedied, then the betterment of that available information service will be depicted by the betterment of the indicator value.

5 Discussion and Conclusion

Aiming to provide a natural explanation of the value of the RiskSOAP indicator, if all 205 absent system element (see Table 3) are approved by the designers of the original system and finally implemented, then the value of the RiskSOAP indicator will turn to ‘0’. Zero distance corresponds to zero deficiencies and means that the system is fully self-aware of the threats and vulnerabilities that can be detected by STPA and EWaSAP. It also implies that the system with the above modified composition has full possession of the risk SA provision capability and its risk DSA is expected to emerge in a greater extent, compared to the system composition as it was involved in the Überlingen accident.

In practice, since ideal system design versions are almost a utopia due to trade-offs, the designers of the system under investigation can set a threshold value for a satisfactory RiskSOAP indicator to determine the modifications that will best suit real-life conditions. Their decision will be probably based on the available resources, i.e. time, budget, available technology, and human operators. If, for example, the threshold is subjectively set at 0.5, the aim will be to obtain an indicator value lower than, or at least equal to, 0.5. Roughly meaning that the secondary aim is to decrease the distance by 0.3471. Simply put, because the value of 0.8471 exceeds the threshold set by the designers, this illustrates that no satisfactory level of risk SA provision capability has yet been reached. This entails an analogous assessment of risk DSA which, according to the original design composition and the designers of the system, can be further enhanced.

To conclude, this paper presented the RiskSOAP methodology accompanied by its corresponding indicator, aiming to facilitate the measurement of a system’s risk SA provision capability and the assessment of its risk DSA. RiskSOAP is based on a verified hazard analysis leading to safety requirements and is also applicable in dynamic systems. Namely, it is easy to readjust the compared units, e.g. parts, subsystems, systems, by improving their design requirements and then recalculate their dissimilarity; just like it happened in the above case of setting a threshold value for the RiskSOAP indicator. All in all, RiskSOAP departs from the notion that a system has its fixed and predefined elements. It is harmonised, though, with the idea that it is feasible to reassess and amend the utility and influential role of system elements in the enhancement or degradation of the system’s risk SA provision capability, even from the early design stages, before the system is booted.

It is worth mentioning that in order for one to take the steps required for STPA and EWaSAP methods, he has to be experienced, well qualified, and supported by a team of interdisciplinary, but with mutual and complementary understanding, researchers.

With a view to draw a conclusion about the risk SA provision capability and risk DSA, the subjective interpretation of the value of the indicator is inevitable. That is, setting a threshold value for this indicator, as discussed in the beginning of this section, may be considered as a limitation of the RiskSOAP methodology because it may differ from system to system and from designer to designer, affecting the degree of design modifications. Another limitation is the overabundance of dissimilarity measures that hinders the decision to select the suitable measure towards achieving the goals set by researchers.

Moreover, here it is neglected that the variables may have a truth value that ranges in degree between '0' and '1'. Acknowledging the limitation of using binary data used herein, future work is intended to involve fuzzy logic, to cope with crisp variables, and adopt continuous variables instead. Weights can also be assigned to the explanatory system elements since, in this paper, they are treated as equivalent to the risk SA provision capability enhancement or degradation.

RiskSOAP can be used a selection criterion between alternative designs of the same or different systems or as decision-making tool between alternative systems. As a further proof of its generality, additional engineering applications and studies are already under consideration.

References

1. Endsley, M.R.: Toward a theory of situation awareness in dynamic systems. Hum. Factors Ergon. Soc. **37**(1), 32–64 (1995)
2. Salmon, P.M., Stanton, N.A., Walker, G.H., Jenkins, D., Ladva, D., Rafferty, L., Young, M.: Measuring situation awareness in complex systems: comparison of measures study. Int. J. Ind. Ergon. **39**(3), 490–500 (2009)
3. Salmon, P.M., Stanton, N.A., Walker, G.H., Jenkins, D.P.: Distributed Situation Awareness: Theory, Measurement and Application to Teamwork. Ashgate, Aldershot (2009)
4. Salmon, P.M., Stanton, N.A., Walker, G.H., Baber, C., Jenkins, D.P., McMaster, R., Young, M.S.: What really is going on? review of situation awareness models for individuals and teams. Theor. Issues Ergon. Sci. **9**(4), 297–323 (2008)
5. Smart, P.R., Bahrami, A., Braines, D., McRae-Spencer, D., Yuan, J., Shadbolt, N.R.: Semantic Technologies and Enhanced Situation Awareness (2007). http://eprints.soton.ac.uk/264351/
6. Stanton, N.A., Stewart, R., Harris, D., Houghton, R.J., Baber, C., McMaster, R., Salmon, P. M., Hoyle, G., Walker, G.H., Young, M.S., Linsell, M., Dymott, R., Green, D.: Distributed situation awareness in dynamic systems: theoretical development and application of an ergonomics methodology. Ergonomics **49**(12–13), 1288–1311 (2006)
7. Stanton, N.A.: Representing distributed cognition in complex systems: how a submarine returns to periscope depth. Ergonomics **57**(3), 403–418 (2014)
8. Chatzimichailidou, M.M., Protopapas, A., Dokas, I.M.: Seven Issues on Distributed Situation Awareness Measurement in Complex Socio-technical Systems. In: 5th International Conference on Complex Systems Design & Management, pp. 105–117. Springer (2015)
9. Chatzimichailidou, M.M., Stanton, N., Dokas, I.M.: 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. Saf. Sci. **79**, 126–138 (2015)
10. Stanton, N.A., Chambers, P.R.G., Piggott, J.: Situational awareness and safety. Saf. Sci. **39** (3), 189–204 (2001)
11. Fioratou, E., Flin, R., Glavin, R., Patey, R.: Beyond monitoring: distributed situation awareness in anaesthesia. Br. J. Anaesth. **105**(1), 83–90 (2010)

12. Leveson, N.: Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, Cambridge (2011)
13. Dokas, I.M., Feehan, J., Imran, S.: EWaSAP: an early warning sign identification approach based on a systemic hazard analysis. Saf. Sci. **58**, 11–26 (2013)
14. Zhang, B., Srihari, S.N.: Binary vector dissimilarity measures for handwriting identification. In: Electronic Imaging, International Society for Optics and Photonics, pp. 28–38 (2003)
15. Nunes, A., Laursen, T.: Identifying the factors that contributed to the überlingen midair collision. In: 48th Human Factors and Ergonomics Society Annual Meeting, pp. 195–198. SAGE Publications (2004)
16. German Federal Bureau of Aircraft Accident Investigation (BFU). http://www.bfu-web.de/EN/Publications/Investigation%20Report/2002/Report_02_AX001–1-2_Ueberlingen_Report.pdf?__blob=publicationFile
17. Johnson, C.W.: Final Report: Review of the BFU Überlingen Accident Report. Contract C/1.369/HQ/SS/04 to Eurocontrol, http://www.dcs.gla.ac.uk/~johnson/Eurocontrol/Ueberlingen/Ueberlingen_Final_Report.PDF
18. Wong, B.: A STAMP Model of the Überlingen Aircraft Collision Accident. MIT Press, Cambridge (2004)