View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by INRIA a CCSD electronic archive server

Degraded situation awareness risk assessment in the aerospace domain

Jean-Marc Salotti, Ephraïm Suhir

To cite this version:

Jean-Marc Salotti, Ephraïm Suhir. Degraded situation awareness risk assessment in the aerospace domain. IEEE International Workshop on Metrology for AeroSpace, Jun 2019, Torino, Italy. hal-02162283

HAL Id: hal-02162283

https://hal.archives-ouvertes.fr/hal-02162283

Submitted on 21 Jun 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Degraded situation awareness risk assessment in the aerospace domain

Jean-Marc Salotti

1: Univ. Bordeaux, CNRS, Bordeaux INP, IMS, UMR 5218, F-33400, Talence, France

2: INRIA, IMS, UMR 5218, F-33400, Talence, France

Jean-marc.salotti@ensc.fr

Ephraim Suhir

1: Portland State University, Depts. of Mech. and Mat., and Elect. and Comp. Engineering, Portland, OR, USA;

2: Technical University, Dept. of Applied Electronic Materials, Inst. of Sensors and Actuators, Vienna, Austria;

3 :ERS Co., 727 Alvina Ct., Los Altos, CA 94024, USA, tel. 650.969.1530, e-mail: suhire@aol.com

***Abstract*—Numerous accidents are due to situation awareness degradation. However, as there exist many different causes and human factors are not well understood, it is very difficult for experts to provide probability risks assessments. It is proposed here to simplify the problem by classifying accidents according to the main demons that degrade situation awareness and to use a Bayesian approach with the Noisy-Or nodes. Interestingly, it is possible to use the same approach in the robotics domain.**

Keywords—situation awareness, Bayesian network, probability risk assessment

I. Introduction

Numerous Human Reliability Analysis (HRA) methods have been proposed to identify and analyze the causes and consequences of human errors [2,3,5,13,16,17]. These methods, based for instance on HFACS methodology (Human Factors Analysis and Classification System [3]) or on a computational model [13], sometimes offer a way to quantify human error probabilities and to provide Probability Risk Assessments (PRA), see Fig.1.

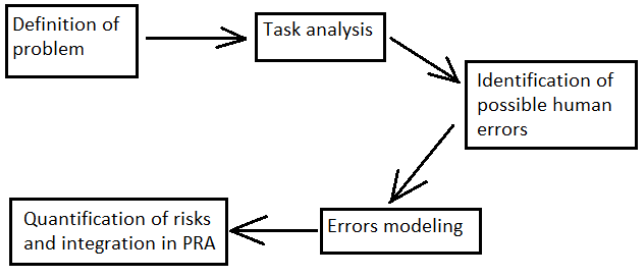

Fig.1: Standard approach for Probability Risk Assessment.

Bayesian belief networks are typically used to this end [1,7,8]. According to Pearl, "Belief networks are directed acyclic graphs in which the nodes represent propositions (or variables), the arcs signify direct dependencies between the linked propositions, and the strengths of these dependencies are quantified by conditional probabilities" [11]. An important difficulty is to choose the variables. Most HRA methods are based on the characterization of Performance Influencing Factors (PIF) to represent the causes of human errors [7,8]. However, human errors are generally associated to the degradation of situation awareness, which is a complex concept making it difficult to define PIF. Different methods are proposed in the literature to take Situation Awareness (SA) into account [1,5,6,15]. Several well-known accidents in aeronautics and astronautics have been examined from the point of view of human factors and situation awareness (SA) degradation [3,5]. Endsley proposed a model of human decision and situation awareness based on different factors that affect perception, action or anticipation [6,17]. However, probabilistic risk assessment linked to SA degradation is difficult because accidents are very different and statistical studies cannot easily be implemented.

In a recent paper, a model based on Bayesian networks has been proposed [14]. The nodes of the network are typical SA demons as suggested by Endsley [6]. Several questions remain open. First, as SA demons are very general, is it possible to use the same risks estimates in different domains? For instance, is it possible to use the same PRA to predict risks accidents in aeronautics, in astronautics and in robotics? Second, what is the reliability of the resulting PRA? And third, after each accident, an analysis is performed, some systems are modified, procedures are evolving and new training scenarios are defined, which should reduce specific risks. How to take these modifications into account in risks estimations? In this paper, we propose to perform a human factor analysis on past accidents in aeronautics and astronautics in order to illustrate the methodology, better understand these issues and make recommendations. Section II, the main principles of the model are recalled. Section III, several accidents are analyzed according to their link to situation awareness degradation. The objective is to identify which SA demon is involved in each case. Section IV, the PRA methodology is presented and the main issues are discussed.

II. Situation Awareness Model

In Endsley's model, 8 SA demons are defined [6]:

- A typical "attentional tunneling" error occurs when an operator has a strong focus on a specific problem, with poor attention to other important parameters, which have to be taken into account to avoid an accident.
- An "out-of-the-loop" syndrome occurs when an automatic system performs a complex task and suddenly gives the control back to a human, who was not following the task and is therefore not able to handle the situation.
- An "errant mental model" may be the root cause of an accident when a human has a wrong interpretation of

the current situation due to inappropriate inferences from observations.

- A "complexity creep" typically occurs when a problem is encountered and there are so many systems involved that the operator is not able to infer any useful conclusion to solve it.
- A "misplaced salience" can be the root cause if the interface of the system is designed to maximize the perception and attention of the user on a specific device, while the salience should be placed on other devices.
- A "Data overload" problem occurs when too many data have to be set or taken into account in a situation with important attentional or time constraints.
- A requisite memory trap occurs when too many subtasks have to be performed and the operator forget one of them.
- An important "workload, fatigue, or stress" has obviously a direct impact on performance and may be the cause of an accident.

See Fig.2 for the Bayesian network with the 8 SA demons. Conditional probabilities can be estimated by human factors experts but there is a lack of methodology and the resulting network is based on empirical assessments [12,14].

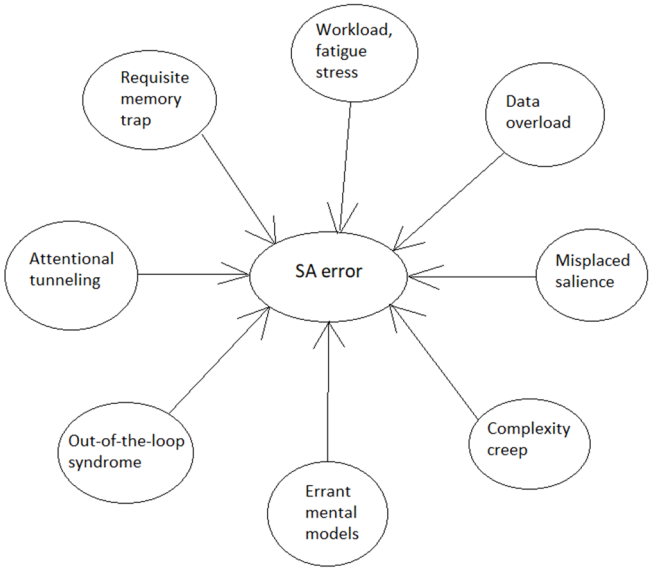

Fig.2. Situation awareness demons.

III. Accidents Analysis

A. *Turkish Airlines Flight 6491*

The flight was operated in January 16th 2017. A thick fog was present at destination. The crew tried to land using instruments until very low "decision height". As they reached the minimum height without visibility, they decided a go-around procedure but the altitude was too low and the plane crashed just behind the runway. The crew failed to determine and follow the appropriate landing procedure for the landing of that specific plane on that specific runway under the specific meteorological conditions. The human error therefore occurred early in the preparation phase. Determining the appropriate decision height from charts and procedures for landing is difficult when there are many different cases. A complementary problem is the wrong mental model of the current situation. As the complexity of the procedure is one of the key problems here, the cause of the accident can be categorized into the "Complexity creep" and "Errant mental" SA issue.

B. *Indonesia AirAsia Flight 8501*

The flight was operated in December 28th, 2014. Three times, the crew had to proceed according to a specific procedure to switch off an alert system. The fourth time, the crew decided to follow a forbidden procedure by switching off the flight augmentation computer, with the unexpected consequence of losing autopilot capabilities (alternate law mode). Later on, a miscommunication between the crew led to opposite commands and the loss of control of the plane. For this specific accident, there are several causes: misplaced salience (3 times amber light alert) and out-of-the-loop syndrome with alternate law mode.

C. *TransAsia Airways Flight 222*

The flight occurred in July 23rd 2014. There were rainy conditions with poor visibility during descent before landing. The crew decided to fly lower than the minimum limit and finally disengaged autopilot. While the plane was approaching the destination, the crew concentrated on the visual search of the runway but there was a small deviation of the trajectory and they missed it. As they did not pay enough attention to the altitude, the plane finally crashed against a hill located behind the airport. The accident was categorized in "controlled flight into terrain". When questioning the company, it was observed that several crews were used to go lower than the admissible limit when the visibility is low. It was also found that the crew had too many flights to operate in a short period of time. The fatigue was therefore a contributing factor. This accident can be categorized in the attentional tunneling and fatigue SA problems.

D. *Luca Parmitano's EVA*

Lucas Parmitano, Italian astronaut, performed an extravehicular activity outside the International Space Station in July 2013. During his EVA, some water was observed in his helmet. It took several minutes for mission control to understand that the problem was serious and to admit that the astronaut had to abort the EVA and urgently come back into the station. He came back safely but he was nearly drowned when he put his helmet off. The problem was hard to understand. There are different systems of the spacesuit that use water. As the water could typically come from a leaky drink bag located close to the head, most experts thought that the problem was minor and did not take appropriate decisions (wrong mental model). After investigation, it was found that the water originated in fact from a cooling system, which was hard to anticipate due to the complexity of the thermodynamic phenomenon that was at work and the wrong belief that the water could only come from the drinking bag. This incident can therefore be categorized in the "complexity creep" and "errant mental model" SA problems.

IV. Probability Risk Assessement

A. Main principles

To summarize, for the Turkish Airlines Flight 6491 accident, the cause is linked with two SA demons: complexity creep and errant mental models; for Indonesia AirAsia Flight 8501, a misplaced salience and a typical out-of-the-loop syndrome have been observed; for TransAsia Airways Flight 222, attentional tunneling and fatigue are involved in the SA degradation; for Lucas Parmitano's incident during EVA outside the International Space Station, the complexity creep and the errant mental model also are at the root causes. These examples clearly show that several situation awareness demons are often observed simultaneously in aerospace accidents. If providing probability risk assessment for a single SA demon is already an issue, providing estimates for the occurrence of several SA demons at the same time is almost unfeasible. In order to simplify probability distributions estimates, and providing that the demon causes are independent from each other, it is possible to use the Noisy-Or framework [9,11,12,14]. The formula is presented below (equation (1).

$$P(\overline{SA}/X_1 \dots X_n) = 1 - \prod_{i=1}^{n}(1 - P(\overline{SA}/X_i)) \qquad (1)$$

If the SA demons are independent from each other, it is indeed not necessary to determine complex conditional probabilities with several variables. The probability can directly be inferred from the product of elementary probabilities.

In order to determine risks estimates of situation awareness degradation, two methods are possible:

- First, risks can be determined by human factors experts. As it is usually performed in typical human reliability analysis, the idea is to list all possible human errors as well as their causes and contexts and to determine the probability of occurrence according to their expertise of the domain. Then, each human error is associated to a SA demon (eventually to several SA demons, depending on context) and probabilities are summed up for each SA demon.
- Second, as it is proposed in this paper, a database of accidents can be analyzed with a specific focus on SA demons:
    - List all accidents (plus all serious incidents). Here, it is suggested to look at accidents in the aerospace domain, but the approach can be generalized to other domains such as robotics.
    - For each accident, if human factors are involved, determine the SA demon(s) that is the root cause.
    - List all accidents involving the same unique SA demon to calculate the probability of occurrence.

B. PRA updates

In practice, however, the rules are often evolving (after an accident, a procedure is often changed to reduce the risk that a similar accident occurs in the future). In order to take that evolution into account, it is possible to reduce the probability according to an arbitrary method. It is proposed here to use a maturity model, which is linked to the number of times an accident is observed (equation 2). A similar model has already been used to take the evolution of an expert's skill into account [14].

$$P(x) = P_{max}(x) + (P_i(x) - P_{max}(x)) \times ((n_0 - n)/n_0)^k \qquad (2)$$

where: P(x) is the probability of not observing x (a specific SA demon) after n modification of procedures
$P_{max}(x)$ is the final probability of not observing x
$P_i(x)$ is the initial probability of not observing x (if n=0 $P(x)= P_i(x)$)
n_0 is the number of new procedures to achieve P_{max}.
k is a decay constant

The idea of the maturity model is to start with an ad hoc estimate of the risk $P_i(x)$, and then to take into account each accident by increasing the probability that the same SA demon is not observed (assuming that something is done to prevent the exact same situation). The probability should slowly increase towards a threshold $P_{max}(x)$, ideally equal to 1, but as nobody is perfect and it is never possible to achieve 100% reliability, the threshold is certainly lower than 1.
Let us illustrate the method with a fictive case. For example, the probability of observing an accident caused by the "out-of-the-loop syndrome" is estimated at 10^{-6} and a new procedure is implemented to reduce the risks. Let us assume that experts believe that we will never reduce the risks below 10^{-7}, 10 additional procedures will probably have to be defined and implemented to achieve that risk level, and k is equal to 2. The new probability can therefore be calculated, it is 8.29×10^{-7}. A graph is also proposed to illustrate the reduction of the risks (see Fig. 3).

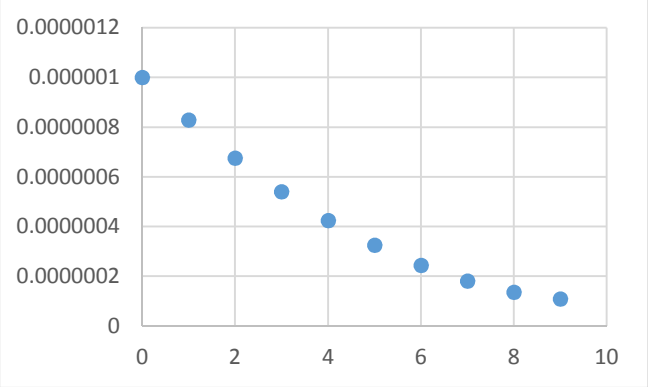

Fig. 3: Update of risks.

It is difficult to determine all parameters a priori. However, the advantage of our approach is that SA demons are very general. It is therefore suggested to look at past accidents with other systems (here other planes or spaceships) and eventually in other domains like robotics. See next subsection.

C. Extrapolation to other domains

It is interesting to look at accidents that occurred in the domain of robotics because there are many similarities between planes and robots and the use of these systems. In aeronautics, autopilots are very common and there are many problems linked with human systems interactions, inappropriate procedures or attentional issues. In the industry

domain, many robots are used. These robots are in general autonomous, are able to perfume a long sequence of complex tasks and are therefore comparable to autopilots. Accidents in robotics are often linked to inappropriate maintenance procedures, failure to understand the state of the robot and attentional problems. Let us present and discuss examples taken from the Occupational Safety and Health Administration database of the United States Department of Labor:

- « At 1:30 a.m. on January 17, 2017, Employee #1 was operating a forklift, removing stacked and wrapped bag pallets from a pallet wrapper. A Fuji-Ace Mechanical Robot was used to load pallet bags onto wood pallets on a conveyor, which moved the loading stack to a pallet wrapper. When completed, the employee then moved the plasticized pallet to storage within the facility. The employee witnessed the robot arm that was feeding pallet bags onto the wood pallets on the conveyor, strike a pallet bag, loosening a hose on the robot hand and causing a mechanical issue that stopped the loading process. Employee #1 climbed onto the stopped conveyor and walked into the caged robot arm area to reconnect the loose hose on the robot's hand. As he proceeded toward the hose, the robot arm engaged, striking Employee #1 in the chest area, and causing a broken sternum and 2 broken ribs. The employee was hospitalized and treated for his injures ». In this case study, there is clearly a situation awareness error. Though the motivation of the employee is not clear, he was probably convinced that the robot was automatically stopped. Two SA demons may be involved here. The first is "Out of the loop syndrome", because the employee didn't know exactly the state of the robot. A second SA demon is "Errant mental model" because the employee had the feeling that he could simply solve the problem without following safety procedures.

- « On January 15, 2002, Employee #1, a maintenance technician for Xilinx Corporation, was performing normal maintenance on a Seiko Epson Handler scanner. He removed a side door to improve access and finished with the adjustments. While test running the machine from in front and watching the operation, he inadvertently reached up and rested his hand on the frame of the unit. His fingers slipped into the opening, and the robot carriage head moved toward the front. The outside edge of the head became caught and pinned his right index finger between itself and the frame, amputating the finger between the first and second knuckle. The hazard was not recognizable. » In this case study, there is also a typical SA error. As the attention of the employee was focused on the operational test and not on the position of his hands, the main SA demon involved in this SA error is "Attentional tunneling".

According to Dhillon [3], "the largest proportion of major injuries or deaths takes place when debugging or unsnagging a robot system and its interfacing devices. Some of the reasons for these accidents are:
(i) Workers frequently take chances as opposed to following the prescribed procedures fully.
(ii) Workers often forget about hazards associated with a robot under normal or abnormal conditions.
(iii) Workers become preoccupied and self-satisfied."
These 3 reasons are typically encountered in the aerospace domain and are closely linked to situation awareness issues. As previously illustrated, in most robotics accidents, SA demons can easily be identified and are clearly very similar to accidents encountered in aeronautics. For these reasons, it is expected that PRA based on SA demons might be very similar and if a hierarchy of SA demons is performed according to its probability of involvement in accidents, it might well be the case that the same hierarchy would be obtained in both domains.

V. Conclusion

It is proposed here to help human factors experts to perform a situation awareness degradation risk assessment. It is based on Endsley's model of situation awareness, Bayesian networks and a methodology based on the experience gained with the knowledge of past accidents and a maturity model that takes into account the improvement of interfaces, procedures and training. Several methods, based on HFACS model, already exist and provide PRA, but they can be improved using our model, which is focused on SA demons. In order to calculate conditional probabilities, a careful analysis of past accidents can be undertaken. Human factors experts can eventually propose their own predictions, based on their understanding of the risks, taking into account PRA in robotics.

References

[1] C. Baoping, L. Yonghong, Z. Yunwei, F. Qian, L. Zengkai and T. Xiaojie T. "A dynamic Bayesian networks modeling of human factors on offshore blowouts", in Journal of Loss Prevention in the Process Industries, Vol. 26 No. 4, July 2013, pp. 639-649.

[2] G.Z. Bedny, W. Karwowski, I.S. Bedny. "Applying Systemic-Structural Activity Theory to Design of Human-Computer Interaction Systems", Boca Raton, Florida, USA, CRC Press, Taylor and Francis Group, 2018.

[3] S. Chapell et al, Human Error and Commercial Aviation Accidents: An Analysis Using the Human Factors Analysis and Classification System, Human Factors,Vol. 49, No. 2, April 2007, pp. 227–242.

[4] B. S. Dhillon, Robot Reliability and Safety© Springer-Verlag New York, Inc 1991.

[5] M. R. Endsley and D.J. Garland (Eds.)" Situation awareness analysis and measurement", Mahwah, NJ: Lawrence Erlbaum, 2000.

[6] M. R. Endsley and D. J. Jones, "Designing for situation awareness: An approach to user-centered design" (2nd ed.), London: Taylor & Francis, 2016.

[7] K. Groth and A. Mosleh, "Development and Use of a Bayesian Netowrk to Estimate Human Error Probability", proceedings of the International Topical Meeting on Probabilistic Safety Assessment and Analysis Wilmington, NC, USA, March 13-17, 2011.

[8] K. M. Groth and A. Mosleh, "Deriving causal Bayesian networks from human reliability analysis data: a methodology and example mode", Proc Inst MechEng, Pt O: Journal of Risk Reliability, vol. 226 (4), 2012, pp. 361–79.

[9] J. F. Lemmer and D. E. Gossing "Recursive Noisy OR—A Rule for Estimating Complex Probabilistic Interactions", in IEEE Transactions on Cybernetics, Vol .34 No. 6, January 2005, pp. 2252 – 2261.

[10] L. Mkrtchyan and V. N. Podofillini, "Bayesian belief networks for human reliability analysis: A review of applications and gaps", in Reliability Engineering & System Safety, Vol. 139, 2015, pp. 1-16.

[11] J. Pearl ,"Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference", Morgan Kaufmann, 1988.

[12] J. M. Salotti, "Noisy-Or nodes for conditioning models", in Lecture Notes in Artificial Intelligence, Vol. 6226, pp. 458-467, Springer, from "Simulation of Adaptive Behaviors", (SAB 2010), Paris, 24-28 August, 2010.

[13] J.M. Salotti and E. Suhir, “Manned Missions to Mars: Minimizing Risks of Failure”, in Acta Astronautica, Vol. 93, 2014, pp. 148–161.

[14] J.M. Salotti, Bayesian Network for the Prediction of Situation Awareness Errors, International Journal on Human Factors Modeling and Simulation, Special Issue on: Quantifying Human Factors Towards Analytical Human-in-the-Loop, January 2018.

[15] N. B. Sarter and D. D. Woods, “Situation awareness: A critical but ill-defined phenomenon”, The International Journal of Aviation Psychology, Vol. 1, No. 1, 1991, pp. 45-57.

[16] E. Suhir, “Miracle-on-the-Hudson: quantitative aftermath”, International Journal of Human Factors Modelling and Simulation, Vol. 4, No. 1, 2013, pp. 35-62.

[17] E. Suhir, S. Lini, C. Bey, J.M. Salotti, S. Hourlier and B. Claverie, “Probabilistic modelling of the concept of anticipation in aviation”, Theoretical Issues in Ergonomics Science, Vol. 1, No.1, 2015, pp. 69-85.