

Human-Centred Automation of Threat Evaluation in Future Fighter Aircraft

Tove Helldin, Göran Falkman
tove.helldin@his.se, goran.falkman@his.se

Informatics Research Centre
University of Skövde
Box 408
SE-54128 Skövde

Abstract: It has long been considered crucial to develop decision support systems that aid fighter pilots achieve their goals. Such systems often require automation of tasks formerly performed manually by the pilots, in situations characterized by huge amounts of (possibly uncertain and incomplete) sensor data and contextual information, time-pressure and dynamically changing tasks. Thus, careful investigations must be performed so as to develop such systems that provide accurate support for their users. This paper reports on the findings concerning research within the field of human-centred automation as well as presents empirical results concerning the applicability of automation guidelines when designing information fusion based support systems in the fighter aircraft domain.

1 Introduction

The implicit aim of most information fusion applications is to support their users when performing tasks or making decisions (see for instance [Bos06, BFSL99]). This is highlighted by the introduction of the level 5 of the JDL model (cognitive refinement) where emphasis is put on successful interaction between the information fusion system and the human operator to improve the decision making process [HM04]. Since the 1980's, there have been several efforts to improve the pilots' execution of their tasks, mostly through the introduction of different support systems. This trend is anticipated to be prevalent also in the future of military aircraft – in pace with the introduction of new, improved sensors and weapons, additional support must be provided to the pilots in order for them to achieve their goals and perform their tasks in a domain characterized by large amounts of (possibly uncertain and contradictory) data, high physical and mental workload as well as enormous time-pressure. Furthermore, additional complexity is added through the introduction of extended teams consisting of both manned and unmanned vehicles that must cooperate. In [EHN10], the challenges and opportunities for developing a threat evaluation decision support system that automatically evaluates and prioritizes threats in a fighter pilot team setting is presented. However, decision support systems often incorporate fully automatic or semi-automatic functions that take over all or some of the tasks formerly

performed manually by its users, of which both positive and negative effects have been reported. Thus, careful investigations must be performed so as to develop automated or semi-automated decision support systems that appropriately support their users. In light of these observations, research within the field of human-centred automation has flourished (see for instance [Ina06, SS⁺04]), where the aim is to develop automated support systems that work in collaboration with the human user – not replacing him/her.

This paper reports on the findings concerning research within the field of human-centred automation in relation to a proposed information fusion based threat evaluation support system. The applicability of identified human-centred automation guidelines, developed to appropriately calibrate trust in the automated functions as well as to support effective cooperation between fighter pilots, is investigated within a threat evaluation setting. Results indicate that the majority of the identified human-centred automation guidelines are applicable in the fighter aircraft context, however with some modifications. The results presented are anticipated to provide guidance for developers of information fusion decision support systems in relation to human-centred automation.

2 Human-centred automation

In pace with the cumulative introduction of automated technologies in various domains with the, often implicit, aim of decreasing operator workload and increasing operator situation awareness (i.e. the same aims as the ones posed in relation to the introduction of the level 5 of the JDL model ([BP02])), researchers have acknowledged the fact that these technologies must be developed with the human operator in mind. Human-centred automation is an approach to create an environment in which humans and machines collaborate cooperatively [Bil97]. According to Billings [Bil97], general principles of human-centred automation constitute, amongst others, the incorporation of the human operator in the execution of the automated tasks, appropriate information distribution as well as automated functions that are easy to learn and to operate. Related research areas include (intelligent) adaptive aiding systems that, for example, adapt which tasks to automate according to the current situation as well as mixed-initiative approaches in which efficient collaboration between the human operator and the automated systems are strived for [HGB07, IBKB10].

Three important aspects to consider when developing support systems suitable for their users are the amount of trust the users have in the automated functions, which tasks that are suitable to automate and at which level of automation these should be implemented. Furthermore, knowledge of positive and negative effects of introducing automated technologies in the users' working environments is also important. These aspects are the focus of the following sub-sections.

2.1 The issue of trust

Several definitions and characteristics of human-centred automation have been proposed and it has been suggested that the features of such systems must be adapted according to the specific domain in mind [Ina06]. However, the amount of trust the operator has in the automated system has been recognized as a general important characteristic of successful human-centred automation [ADR06, LS04, RMP07, SB08]. Madsen and Gregor have defined trust in human-machine systems as *'the extent to which a user is confident in, and willing to act on the basis of the recommendations, actions and decisions of an artificially intelligent decision aid'* ([MG00]) (p.1). Thus, trust is a multifaceted concept, incorporating both psychological and technical issues. According to [AS09], the issue of trust is becoming increasingly important in pace with the development of new user supporting technologies since it is *'potentially harder to gain, easier to loose and even more difficult to recover when lost'* (p.161).

2.2 Tasks and levels of automation

Not only must the human-centred automation designer take the issue of trust into account when designing support systems, but he/she must also carefully select which tasks to automate. In most domains, there are several tasks that automated functions can be designed to perform. According to Parasuraman et al. [PSW00], there are four broad classes of functions that automation can be applied to, namely information acquisition, information analysis, decision and action selection and action implementation. Information acquisition can involve strategies for mechanically directing sensors in order to observe a specific geographic area. It might also include an organization or highlighting of incoming information from such sensors according to some criteria. Automation of information analysis might imply presenting analyses of projected future states of objects, the aggregation of several variables to a single variable or present context dependent summaries of data to the user. Decision and action selection might involve the generation of system recommendations of what the user should decide, while automation of action implementation might imply the support system's execution of the selected action.

Table 1: A ten-point scale of levels of automation (adapted from Sheridan et al. [She78])

Low	1	The computer offers no assistance, humans must perform all decisions and actions
	2	The computer offers a complete set of decision/action alternatives
	3	Narrows the selection down to a few
	4	Suggests one alternative
	5	Executes the suggestion if the human approves to
	6	Allows the human a restricted time to veto before automatic execution
	7	Executes automatically, then necessarily informs the human
	8	Informs the human only if asked
	9	Informs the human only if the computer decides to
High	10	The computer decides everything, acts autonomously, ignoring the human

An additional important characteristic of successful human-centred automation is the level of automation (LOA) implemented [PSW00, RMP07]. According to Sheridan et al. [She78] there are ten different levels of automation, ranging from low automation (i.e. manual control) to high automation (see Table 1). In relation to the different automation levels, Banbury et al. [BGS⁺07] argue that automated systems should improve, rather than replace, the operator's decision making ability. Such recommendation might be met by the incorporation of a lower level of automation, as well as by providing informative feedback to the operator, informing him/her of the tasks performed by the automated system. The LOA need not be fixed in the system design but might be adapted according to the evolving situation. However, as argued in [PSW00], careful investigations must be performed so as to provide the correct type and appropriate level of automation in the domain of interest.

2.3 Pros and cons of automation

The introduction of automated technologies might result in both positive and negative effects. Amongst the positive effects, Parasuraman et al. [PSW00] argue that automation can improve an operator's awareness of the situation and ease an operator's mental workload by, for example, letting automation perform repetitive tasks ill-suited for human operators. As such, the operator can spend more time on tasks requiring deeper analysis and specific operator expertise. In relation to the categories of automation tasks, this could imply a high level of automation of tasks such as information acquisition and analysis, as well as a low level of automation of decision and action implementation tasks. An example of successfully implemented autonomous functions can be found in Rovira et al. [RMP07] where improved operator performance was reported when automating the task of identifying the most threatening object in a command and control setting (i.e. high automation of information acquisition and analysis). However, researchers have also identified negative effects of automation. One example can be found in the civil aircraft domain where the pilots of one Airbus A320 aircraft over-trusted the autopilot of the aircraft, leaving them no time to take manual control so as to avoid the collision with the ground [LS04]. Parasuraman and Riley [PR97] have documented that inappropriate automation can result in misuse, disuse and abuse of automated functions not intended by the designer. Such ill-designed automation might increase the mental workload of an operator if he/she, for example, does not understand how the automated system works or what is being performed.

Automation might also decrease an operator's awareness of the situation by alienating him/her from the tasks carried out (i.e. a too high LOA, see Table 1), leaving the operator less attentive to changes in the environment caused by the autonomous functions [PSW00]. Functions that leave the operator as a mere observer could also result in skill degradation and a sense of being positioned out-of-the-loop. A highly reliable, but not 100% perfect system might also lead to operators having trouble to detect automation failure when it does occur [PSW00].

In relation to trust, experiments have shown that trust in automated systems decreases if failures are performed on easy tasks, in contrast to more difficult tasks. Trust has also been shown to depend on the risks involved - the higher the risk level, the larger amount of

trust is required for the operator to use the system. This may lead to unwarranted distrust, unnecessary monitoring and overriding of good decisions [ADR06]. Thus, the result of not analysing the potential positive and negative effects of automation as well as carefully design the autonomous functions might have severe effects on operator trust as well as on operator performance.

By considering issues such as how to correctly calibrate the amount of trust the operator should have in the automated functions, which tasks should be automated as well as at which level of automation these tasks should be implemented during the design process, negative consequences of automated technologies on operator performance might be prevented and a foundation for positive automation effects might be established.

3 Automation guidelines

To aid developers create automated systems that operators can trust, Atoyan et al. [ADR06] have suggested a set of domain-independent automation guidelines (see Table 2).

Table 2: Trust in automation guidelines (adapted from [ADR06])

1	Provide access to raw data
2	Provide means to indicate to the user that data is missing, incomplete, unreliable or invalid
3	Make clear to the user the purpose of the automation
4	Design with good computer etiquette
5	Reveal the rules and algorithms used by the automation, and if possible, keep the algorithms simple
6	Group and isolate less reliable or vulnerable functionalities of your system if it is possible
7	If algorithms of the system are context dependent, make the context explicit to the operator
8	Show the source of automation failure
9	Provide the user with an adaptable automation
10	Train the operator in order to develop adequate trust
11	Evaluate trust in the system both at the introductory stage and after acquiring a certain level of experience with the system operation

The first guideline advocates that the operator should have access to the raw data used by the autonomous functions in order to enable him/her to check the reliability of the outcomes of these functions. Another way of appropriately calibrating an operator's trust in the automated functions is to indicate when data is missing, incomplete, unreliable or invalid. As such, the operator can perform control tasks in order to compensate for such errors. The third guideline promotes an explicit explanation of why the automation was implemented, i.e. how the automated functions are designed to aid the operators perform their tasks. As such, the operators might be less reluctant to use the aid. However, automated functions should not be designed to appear more reliable than they really are which might lead to, for example, misuse of the automated functions. This is referred to as 'designing with good computer etiquette', as proposed by the fourth automation guideline.

The fifth guideline highlights the importance of giving the operators an insight into the inner workings of the automated functions. As such, they can easier understand the decision process followed as well as why the automation sometimes fails. However, in order to minimize the risk of spreading distrust in one automated function to other such functions, studies have shown that if carefully grouped and isolated, such spread of distrust might be prevented, as suggested by the sixth guideline. The seventh guideline concerns the explicit presentation of the current system "mode" if the algorithms implemented depend on it. As such, the operators' understanding of the work performed by the automated functions might increase. Furthermore, the source of automation failure should be presented to the operators. If a fault has occurred because of, for example, loss of power and not because of the automation itself (software bugs etc.), the operator's trust in the automated functions might be maintained on an appropriate level. The ninth guideline promotes the implementation of adaptive automation to provide appropriate support at appropriate occasions. Of importance is also the training of the operator where he/she is informed of the performance of the automated functions. However, poor design should not be compensated by extensive training. The last guideline asserts that an operator's trust in the automated functions should be evaluated at the introductory stage as well as after having used them for some time.

Additional automation guidelines identified from the work of [ADR06, BGS⁺07, PSW00, RMP07] are added in Table 3. The first one suggested by Atoyan et al. [ADR06] concerns the importance of providing relevant feedback of the tasks carried out by the automated functions. As such the operator's awareness of the situation might be improved. Banbury et al. [BGS⁺07] propose another recommendation to deal with the 'out-of-the-loop' performance problems, which is argued to be possible to prevent by designing the automated functions to be cooperative rather than replacing the operator. The last guideline presented in this paper is proposed by Parasuraman et al. [PSW00] and Rovira et al. [RMP07] who suggest that appropriate LOA:s should be considered when designing the automated functions so as to develop support that is appropriate for its intended users.

Table 3: Additional automation guidelines (after [ADR06, BGS⁺07, PSW00, RMP07])

12	Provide relevant feedback
13	If possible, make the automation cooperative rather than replacing the operator
14	Carefully design the automation with appropriate automation levels in mind

These guidelines are anticipated to aid system designers develop automated functions that support their operators in appropriate ways, with primary focus on operator trust in the automated functions implemented and on appropriate LOA. However, how to design the automation of team-cooperative tasks has, to our knowledge, not been extensively investigated within the fighter aircraft domain. Thus, the following of this paper investigates both the applicability of the automation guidelines, developed to appropriately calibrate operators trust in the automated functions, in the fighter aircraft domain, as well as if additional guidelines can be identified that can support increased and effective cooperation between fighter pilots in a threat evaluation setting.

4 Automation of threat evaluation in the fighter aircraft

The purpose of the threat evaluation process performed by fighter pilots is to determine the level of threat posed by objects in their environment. According to Irandoust et al. [IBKB10], such evaluation should establish the current intent, capability and opportunity of non-friendly entities within the volume of interest based on a priori information and dynamically acquired information. It is thus a continuous process due to the constantly changing environment and there is often no time for the fighter pilots to perform exhaustive analyses taking all available data into account. It has thus been anticipated that a threat evaluation decision support system should be developed to improve the threat evaluation ability of fighter pilots and thus their chances of combat survival [EHN10]. However, in light of findings concerning trust in automation, how should such evaluation system function to support an appropriate calibration of trust in the automated functions? Furthermore, due to the anticipated future increase in team collaboration within the fighter aircraft domain, how could such system be designed to support this increased collaboration within a team of fighter pilots? The next sub-sections present the results from an empirical investigation where fighter pilots were asked to describe how they would like to work and cooperate with a future threat evaluation support system.

4.1 Empirical investigation

A survey was distributed to ten Swedish fighter pilots with experience of the Swedish JAS 39 Gripen aircraft in order to receive their opinions of how automated functions in a threat evaluation scenario should function. Thirty questions concerning appropriate levels of automation, support for teamwork and trust in automation in relation to the development of a new automated threat evaluation system were posed and answered by five pilots through a web based survey tool. The participants were, for example, required to rank on a five point scale how important it is for them to have automatic system support during flight that aid them with tasks such as information acquisition, information analysis and decision and action selection and action implementation in general and in relation to the threat evaluation support system proposed. The pilots were also required to express their opinions of appropriate LOA in relation to the threat evaluation support system described, as well as on specific trust related issues such as if they would like to have access to the raw data used by the support system. Specific tasks to automate to support enhanced team cooperation in a threatening situation were also discussed. Some of the automation guidelines presented in Table 2 and Table 3 received more attention in this study due to their anticipated importance in the fighter aircraft domain and in relation to the proposed threat evaluation support system (see recommendations 1 – 3, 5, 8, 12 – 14). Focus was also put on the different categories of automation tasks identified by Parasuraman et al. [PSW00] to investigate which tasks would be appropriate to automate in a threat evaluation scenario. The questions posed in the survey were first evaluated together with a fighter pilot in order to test their validity in the particular domain. The general conclusions drawn from the survey are presented below.

4.2 Appropriate automation tasks and LOA

In relation to which tasks to automate in a threat evaluation setting, the participants in the study agreed upon that a future threat evaluation support system should aid fighter pilots with generating suggestions of appropriate actions to perform that appropriately mirror the threat situation (i.e. LOA 2 – 4). Such suggestions should then be automatically implemented or rejected based on the pilot's judgment. Important tasks to automate would thus be to gather information from the environment as well as to analyse and make inferences from the information. Additionally, support for generating recommendations based on the collected information was also considered an important task to automate.

Somewhat varied responses were collected regarding tasks that require higher levels of automation, i.e. to automatically perform tasks without the involvement of the pilot himself. However none of the pilots suggested a higher LOA than level 6 (see Table 1). For example, the automation of weapon deliveries was considered to be a task that should be manually performed by pilots, whereas the release of chaffs and flares was considered to be an appropriate task to be highly automated. Thus, the appropriate LOA greatly depends on the specific tasks in mind.

When asked about which LOA to incorporate in relation to the threat evaluation system described, the majority of the participants answered that the evaluation system should offer the pilot a limited amount of time to veto the recommendation posed by the system before the system's automatic implementation of the recommendation (i.e. LOA 6). However, this relatively high level of automation should be looked upon in light of the carefully selected tasks that the pilots argued that the automated functions could provide support to.

The appropriate LOA suggested by the pilots are in line with the suggested automation guidelines 13–14 (see Table 3), arguing that automated functions should be cooperative (and not replace the operator) as well as that careful investigations must be performed so that appropriate tasks are automated at an appropriate LOA.

4.3 Trust in automation

All pilots in the study argued that they have more trust in systems if they have some knowledge of how they function and why they have been implemented (guideline 5 and 3). However, this is something that must be taught during training since there often is no time during a mission to understand a system's inner workings or analyse the raw data fed to the system. Such raw data should instead be analysed after a mission in order to evaluate the performance of the support system (guideline 1). It was furthermore stressed to only automate tasks that would appropriately ease the pilot's working situation to decrease the risk of providing too much automation and, consequently, increase the risk of causing out-of-the-loop performance problems (guideline 13).

To trust the recommendations posed by a threat evaluation system, the pilots argued that it would be very important to receive an indication of how reliable the results from the evaluations are (guideline 2). Furthermore, to have control over the situation and trust the

system used, the pilots participating in the study argued that the support system should inform the pilots of the tasks that it performs (guideline 12)

In safety critical systems, such as those incorporated into an aircraft, the systems must be robust and not susceptible to automation faults. A majority of the pilots in the study argued that they are not able to analyse faults performed by the autonomous functions, if not explicitly apparent in the information presentation. Nor would they have time to analyse the automation failure. Thus, automation faults must be clearly presented to the pilots (guideline 8) as well as their negative consequences limited.

4.4 Cooperative automated functions

Today, the pilots cooperate mostly through the use of radio communication and through the data link between the aircraft in a team. However, in stressful situations with high workload and uncertain information there might be problems with proposing actions to collectively perform as well as to absorb and comprehend the data communicated. Therefore, one of the pilots in the study argued that it would be helpful if the automated threat evaluation support system could generate a set of possible actions, present these to the team leader, and then distribute and execute the suggestion chosen by the team leader. As such, less time could be spent on manually generating suggestions and reduced manual communication would be needed. Furthermore, such arrangement should also involve an automatic update of the team's common situational picture, aiding the team to cooperate more efficiently. This requested team functionality is also in line with the requested LOA for this type of support system where the majority of the pilots in the study argued that a threat evaluation support system should suggest an alternative to the pilot and then allow him/her during a restricted time to veto the suggestion before automatic execution.

The results from the survey also indicate that a general improvement of the team's common situational picture is requested. By fusing data from the different sensors available in a team, a more coherent and correct picture of the environment can be created and maintained, leaving the team of pilots with a good foundation to base its decisions on. Furthermore, one of the pilots argued that to be able to share each other's sensors during flight would also improve the execution of their cooperative tasks during a mission.

Enhanced cooperation within a team would also aid the pilots to easier perform on-the-fly mission planning. In a cooperative scenario, one of the pilots argued that support should be provided that automatically aids the pilots to abort their current tasks in order to save fuel, stay on the same altitude etc., i.e. to "save up" resources for future tasks.

From these empirical findings, an additional automation guideline supporting enhanced cooperation within a team of fighter pilots is proposed that is able to provide automatic support for generating and distributing suggestions of team actions and team relevant information within a team. Another automation guideline identified from the survey performed concerns automatic support for updating the individual pilot's and the team's situational pictures. These additional guidelines are added to the pool of guidelines in Table 4.

5 Discussion

The results from the study performed indicate that most of the automation guidelines described in this paper are directly applicable to the fighter aircraft domain within a threat evaluation scenario. However, due to the often stressful working environment of fighter pilots, raw data used by the proposed threat evaluation support system should not be presented to the pilots during flight. Instead, such information should be provided during training to understand the inner workings of the automated functions, as well as after a mission to evaluate the performance of the automated functions. Furthermore, of utmost importance is to display how reliable the results from the threat evaluation performed are as well as what factors that influence the evaluation.

Additional automation guidelines concerning enhanced cooperation within a team should be added to the suggested pool of automation guidelines to aid human-centred automation developers design appropriate automated team functions. Automatic support to improve information and decision distribution within a team has been identified as important for enhanced cooperation within a team of pilots, as well as automatic support for updating the pilots' individual and collective situational pictures. Table 4 presents the suggested set of automation guidelines which incorporates the previously identified guidelines as well as the guidelines identified from the empirical investigation.

Table 4: Automation guidelines concerning trust and enhanced cooperation in a threatening scenario

1	Provide access to raw data
2	Provide means to indicate to the user that data is missing, incomplete, unreliable or invalid
3	Make clear to the user the purpose of the automation
4	Reveal the rules and algorithms used by the automation, and if possible, keep the algorithms simple
5	Show the source of automation failure
6	Provide relevant feedback
7	If possible, make the automation cooperative rather than replacing the operator
8	Carefully design the automation with appropriate automation levels in mind
9	Provide automatic support to enhance information and decision distribution within a team
10	Provide automatic support that updates the individual and team situational pictures

It is anticipated that the guidelines presented in Table 4 will aid information fusion system designers create systems that successfully support their users' decision making processes through the incorporation of automated functions that increase operator situation awareness and decrease operator workload, i.e. the aim of the fifth level of the JDL model [BP02] and the situation awareness model (as described by Endsley [End00]). If, for example, appropriate feedback from the information fusion based support system is given concerning the tasks that the system performs and the data used, the human operator might be aided with avoiding out-of-the-loop performance problems as well as with improving his/her situation awareness, resulting in a better work environment and a base for making better decisions for the operators.

6 Conclusions and future work

Support systems incorporated into modern fighter aircraft are constantly changing to accommodate for new tasks to be performed and new requirements. These systems often incorporate automatic or semi-automatic tasks to support their users. As documented in this paper, it is of outmost importance to carefully design such support systems so as to suit its users. In this particular domain, characterized by time-pressure, high workload, uncertain data and where wrong decisions might get fatal consequences, the importance of providing appropriate support becomes even more central. This paper has pointed towards the importance of designing the proposed threat evaluation support system with the concept of human-centred automation in mind.

The modified and added automation guidelines are anticipated to provide support for developers of information fusion support systems where issues such as trust in the automated functions as well as team cooperation are of great importance for successful decision making. Future work includes a further evaluation of the identified automation guidelines together with additional pilots and modern fighter aircraft system developers as well as the implementation of a prototype of the proposed threat evaluation support system. The prototype, with founding in the automation guidelines identified, must be evaluated together with fighter pilots so as to receive their opinions of its design in relation to trust in the automated functions, the appropriate level of automation as well as how the automated functions can support enhanced team cooperation within the fighter pilot team.

7 Acknowledgements

This research has been supported by Vinnova through the National Aviation Engineering Research Program (NFFP5- 2009-01315), Saab AB and the University of Skövde. We would like to thank Lars Niklasson (University of Skövde), Jens Alfredson and Tina Erlandsson (Saab Aeronautics) for their useful ideas and our fruitful discussions.

References

- [ADR06] H. Atoyan, J.R. Duquet, and J.M. Robert. Trust in new decision aid systems. In *Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine*, pages 115–122. ACM, 2006.
- [AS09] H. Atoyan and E. Shahbazian. Analyses of the Concept of Trust in Information Fusion and Situation Assessment. *Harbour Protection Through Data Fusion Technologies*, pages 161–170, 2009.
- [BFSL99] A.M. Bisantz, R. Finger, Y. Seong, and J. Llinas. Human performance and data fusion based decision aids. In *Proceedings of the FUSION*, volume 99, pages 918–925, 1999.
- [BGS⁺07] S. Banbury, M. Gauthier, A. Scipione, ON Kanata, and M. Hou. Intelligent Adaptive Systems. *Defence R&D Canada (DRDC) Toronto, CR, 75:269*, 2007.

- [Bil97] C.E. Billings. *Aviation automation: The search for a human-centered approach*. Lawrence Erlbaum Associates Publishers, 1997.
- [Bos06] E. Bossé. An essay to characterise information fusion systems. Technical report, Defence Research and Development Canada Valcartier (Quebec), 2006.
- [BP02] E. Blasch and S. Plano. JDL Level 5 fusion model: user refinement issues and applications in group tracking. In *SPIE Aerosense*, volume 4729, pages 270–279. Citeseer, 2002.
- [EHNf10] T. Erlandsson, T. Helldin, L. Niklasson, and G. Falkman. Information Fusion supporting Team Situation Awareness for Future Fighting Aircraft. In *Proceedings of the 13th International Conference on Information Fusion*, 2010.
- [End00] M.R. Endsley. Theoretical underpinnings of situation awareness: A critical review. *Situation awareness analysis and measurement*, pages 3–32, 2000.
- [HGB07] M. Hou, M.S. Gauthier, and S. Banbury. Development of a generic design framework for intelligent adaptive systems. In *Proceedings of the 12th international conference on Human-computer interaction: intelligent multimodal interaction environments*, pages 313–320. Springer-Verlag, 2007.
- [HM04] D.L. Hall and S.A.H. McMullen. *Mathematical techniques in multisensor data fusion*. Artech House Publishers, 2004.
- [IBKB10] H. Irandoust, A. Benaskeur, F. Kabanza, and P. Bellefeuille. A mixed-initiative advisory system for threat evaluation. 2010.
- [Ina06] T. Inagaki. Design of human-machine interactions in light of domain-dependence of human-centered automation. *Cognition, Technology & Work*, 8(3):161–167, 2006.
- [LS04] J.D. Lee and K.A. See. Trust in automation: Designing for appropriate reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 46(1):50, 2004.
- [MG00] M. Madsen and S. Gregor. Measuring human-computer trust. In *11th Australasian Conference on Information Systems*, volume 53. Citeseer, 2000.
- [PR97] R. Parasuraman and V. Riley. Humans and automation: Use, misuse, disuse, abuse. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 39(2):230–253, 1997.
- [PSW00] R. Parasuraman, T.B. Sheridan, and C.D. Wickens. A model for types and levels of human interaction with automation. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 30(3):286–297, 2000.
- [RMP07] E. Rovira, K. McGarry, and R. Parasuraman. Effects of imperfect automation on decision making in a simulated command and control task. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 49(1):76, 2007.
- [SB08] Y. Seong and A.M. Bisantz. The impact of cognitive feedback on judgment performance and trust with decision aids. *International Journal of Industrial Ergonomics*, 38(7-8):608–625, 2008.
- [She78] T.B. Sheridan. Human and computer control of undersea teleoperators. Technical report, Massachusetts Inst of Tech Cambridge Man-Machine Systems Lab, 1978.
- [SS⁺04] A.B.M. Skjerve, G. Skraaning, et al. The quality of human-automation cooperation in human-system interface for nuclear power plants. *International journal of human-computer studies*, 61(5):649–677, 2004.