The Case for Active Fratricide Avoidance in Net-Centric C2 Systems

John Barnett
U.S. Army Research Institute for the Behavioral and Social Sciences

Combat identification – the discrimination between friendly and enemy units in combat – is becoming more and more important as modern combat becomes more complex. As warfare has evolved, distances between combatants have increased. Engagements have moved from face-to-face close combat, to lines of musket men, to direct fire at the limits of visual range, to beyond visual range (BVR), where friendly and enemy units are represented iconically on display screens. This distance has complicated combat identification and made it more difficult for Soldiers to identify friend from foe.

Net-centric command and control (C2) systems bring additional "distance" because Soldiers see only icons generated by the computer rather than units, vehicles, or individual Soldiers. Instead of seeing things with their own eyes, they must rely on data that has been filtered and processed by an electronic system. Soldiers must trust the system to correctly classify the target and display the correct icon to distinguish between targets, friendly forces, and civilians.

Combat Identification and Fratricide Avoidance

The benefit of combat identification is primarily to prevent fratricide; the accidental attack of friendly forces by other friendly forces. For a number of reasons, fratricide can have a more devastating affect on combat effectiveness, both immediate and long-term, than a similar attack by the enemy. Besides the casualties inflicted and equipment damaged, Soldier morale takes heavy damage as well. Soldier confidence in both leadership and other friendly units drops considerably. Fratricide often causes more destruction than a similar enemy attack because it is essentially the same as an ambush – Soldiers are not prepared to receive attacks from friendly units, and thus are caught unawares. Considerable confusion ensues because of the efforts to identify attacking units and stop the attacks. Fratricide incidents have frequently disrupted planned operations (Shrader, 1982, p. 32).

The consequences of fratricide can have far reaching affects. A fratricide incident that occurred in Europe during World War II between American infantry and armor units caused ill

will between the units. Fights between infantry and tankers occurred in hospitals where casualties were sent, and in rest areas behind the lines (Shrader, 1982, p. 86). Such feuds can have a devastating affect on unit cohesion. In addition, a fratricide incident can reduce combat power by making Soldiers reluctant to fire on the enemy until they have double- and triple-checked their identity (Shrader, 1982, p. 4).

There is currently more emphasis on fratricide prevention because beliefs are changing about the nature of fratricide. It is no longer seen as an unavoidable artifact of warfare, but instead is seen as something that is well worth the effort to reduce to its lowest level. Fratricide can also have detrimental political consequences, especially with a coalition force of different nations. Distrust between the military forces of different nations can weaken the coalition.

There are also both political and operational consequences of the unintentional or incidental injury to civilians or other neutrals, known as collateral damage. Collateral damage can be seen as the corollary to fratricide. Where fratricide is the unintentional targeting of friendly forces, collateral damage is the unintentional targeting of civilians and neutrals. In situations where military forces are trying to build trust with civilians, collateral damage can undermine their efforts.

It should be noted that, as with any safety issue which involves human error, it is unreasonable to believe that fratricide can be prevented entirely. Rather, the objective of fratricide avoidance is to reduce the number of fratricide incidents to the lowest level possible while still maintaining effective combat power. At some point there is a trade-off between safety and effectiveness. As an extreme example, a commander could greatly reduce the probability of fratricide by prohibiting the employment of any weapon for any reason. While this would increase safety, it would destroy the unit's combat effectiveness. Therefore, the ideal fratricide avoidance measures are those which reduce the probability of fratricide while having a minimal effect on combat effectiveness. For this reason, the term "fratricide avoidance" is used as opposed to "fratricide prevention."

Net-centric C2 systems have the potential to both help and hinder combat ID and subsequently fratricide avoidance. On one hand, net-centric C2 operations occur in what is essentially virtual space and are therefore once-removed from the battlespace. This has the potential to make it that much harder to discriminate between friend and foe. On the other hand, the automation inherent in net-centric C2 could be used to support friend-or-foe decisions.

The following section provides a description of common elements of net-centric C2 systems, and a discussion of automation in general, as well as some of the issues involved with human-automation interaction.

Background

Net-Centric Command and Control Systems

There are a number of different net-centric C2 systems used by military services. Although each system has unique features, there are certain similarities among all systems of this type. They all tend to be computer systems linked together over a network, similar to the Internet, and share C2 information between the various nodes. Most transmit information wirelessly, using line-of-site radio or satellite. The workstations and displays may be in fixed or mobile command centers, but may also be in individual vehicles such as aircraft, tanks, infantry fighting vehicles, or smaller vehicles such as jeeps and HMMWVs. User controls and displays often mirror personal computer (PC) workstations, and may in fact be PC or laptop computers connected to a network and running specialized software.

Net-centric C2 systems afloat may connect ship's command centers with other ships and aircraft to coordinate anti-air, anti-surface, and anti-submarine warfare. In the air, net-centric C2 systems typically coordinate the defensive counter-air mission, but may support other missions as well. On land, combat related information is shared between units as well as being distributed to higher and lower echelons.

Individual workstations get their information from a network that is normally providing data continuously. The information from the network is processed and displayed to the operator. Data on friendly forces can come from inputs to the network from friendly units, such as Identification Friend or Foe (IFF) transmissions of aircraft or "heartbeat" signals from ground vehicles. Information on enemy forces is less certain, and is normally either entered manually, or when detected electronically, such as by radar or sonar, the classification as enemy is normally verified by an operator before being released to the network. This chain of information can be interrupted for a number of reasons. Communications failures, problems with the interoperability of different systems, and the inclusion of non-networked forces can make it difficult to get the correct information to the correct display.

Automation Aiding of Fratricide Avoidance

Given that net-centric C2 systems are based in computer networks, automation could be used to provide alerts to operators. These alerts are designed to direct the operator's attention to important information, such as safety and fratricide concerns. Alerting software can monitor the data stream transmitted across the network and provide alerts when certain trigger conditions are met.

The types of alerts available might include, for example, when a ground vehicle is approaching a hazardous area such as a mine field or area contaminated with chemical weapons. Another alert might be when a vehicle strays from it's own unit's area of responsibility (AOR) and into the area of another unit. This situation – straying across unit boundaries – has the potential for fratricide since a vehicle in an unexpected location is usually considered an enemy. In the stress and confusion of combat operations correct identification can be difficult. Therefore, ensuring unit members stay within their own boundaries facilitates fratricide avoidance.

Ideally, the types of automated alerts most needed are those where the human operator has difficulty identifying when dangerous conditions occur. In this case the alert would direct the operator's attention to those conditions. For example, a person might have difficulty remembering the times when a restricted zone, such as a restricted fire area or no-fly area, is active and when it is not. Automation has no such problem, and can assist the user by highlighting the area on the display when it is active, and de-emphasizing it when it is not.

The need for adaptable automation. One of the complexities of designing automated aids, such as automated alerts, is that people have differing requirements of the automation at different times and in different situations, usually depending on the levels of workload and performance stress. During periods of low workload and stress, people tend to become bored and attention wanders. At these times, automation can help direct the user's attention to important information or events they might otherwise miss.

Conversely, during periods of high workload and stress, people's attention tends to focus on a central task or event and disregard other information, even important information. Also, there may be so much information presented to the user that it cannot all be mentally processed. In this case, the task of the automated aiding system is to present important information to the user in such a way that it does not interfere with the user's task, nor does it increase their already overburdened mental workload.

A further consideration is that the relative importance of information presented to the user may change with the situation. Information that the user might consider important during tedious parts of a mission might be trivial during active combat.

Change Blindness

One of the reasons that alerts are necessary is that sometimes people working with a computer display will miss changes that occur in the display, a phenomenon called *change blindness* (Durlach & Chen, 2003; Durlach, 2004). Change blindness can occur for a number of reasons, the most common of which is that the change occurred when the operator was distracted, or during eye blinks or saccades (eye movements). Minor changes in on-screen icons during such distractions can be very difficult to notice.

A number of factors can influence whether the operator notices the change. Icons which move or simulate movement (e.g. blink on-and-off) are more noticeable than static icons (Wickens, 1992, p. 81), and are therefore less likely to be missed due to change blindness. Icons which change color are also fairly noticeable. However, icons which change shape, or are near the periphery of the display, are less salient.

Also, recent research suggests that people are better at correctly detecting item appearance than disappearance. Durlach, Kring & Bowens (in press) found that, once the false alarm rate was corrected for, people correctly detected the appearance of icons on a display more often than they detected the icon's disappearance. This means that, even in a moderately cluttered display screen, unit icons that disappear from the screen due to loss of signal have less of a chance to be noticed by the operator than units that join the net and appear on the screen.

Considerations for the Use of Automation in Fratricide Avoidance

As a form of automation, an alerting system would have many of the benefits and drawbacks of other forms of automation. There are a number of issues to consider when people employ automation. The following section discusses some of the issues relevant to using automated alerting systems to aid in fratricide avoidance.

Automation's Affect on Situation Awareness

Situation awareness (SA) has been defined by Endsley as "the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (Endsley, 1988, 1995, 2000). Lack of SA is frequently cited as the cause of accidents, particularly in aviation (Jones & Endsley, 1996), and

good SA is important to safe driving (Gugerty, 1997). Logically, poor SA would increase the chances of fratricide, while good SA would reduce the chance. For this reason, any method that increases an operator's SA would logically reduce the probability of fratricide incidents.

Alerts can be used to direct the user's attention to important events and hopefully increase SA. If the user happens to miss an important change in the display, through change blindness, for example, an alert can direct the user's attention to the change to ensure the user attends to the important information. In this way, automated alerts can improve the user's SA by guiding the user's attention to important information about the situation.

Automation Affect on Mental Workload and Work Flow

Intrusiveness. The effect of alerts on SA is more complex. If an alert occurs at the wrong time, it can distract the user from more important information and actually contribute to change blindness. If the user is performing a task, it can interfere with the task the operator is performing and can actually degrade performance. An example of such intrusive automation which should be familiar to anyone who uses common office software suites is the animated figure which offers to provide "help" to the user when the software determines the user is performing tasks incorrectly or inefficiently. When the animation appears, it prevents the user from continuing to work on the task and forces the user to attend to the animation. Many users find this frustrating and deactivate the automated help function. While such automated help is valuable in theory, in practice it becomes intrusive.

Sometimes users will expect automated alerts to be useful, but find them to be intrusive in practice. During one experiment of a highly automated future combat system, observers noted that system operators who were allowed to set a number of automated alerts frequently set the majority of the alerts at first, but during operations found them to be intrusive and either ignored or disabled them (P. Durlach, personal communication, March 26, 2008).

How Automation Affects Decision Making

How automation affects people's decision making is not entirely clear. Under certain conditions, automation aids decision making, but under different conditions they make worse decisions (Bowers, Oser, Salas & Cannon-Bowers, 1996). However, one thing that is clear is that when people are presented with decisions by automation, they tend to accept it at face value and curtail any further data collection (Mosier, Heers, Skitka & Burdick, 1997).

Automation Reliability and User Confidence

Automation is often seen as a method for reducing human error. Automated alerts can be used to direct a user's attention to elements in a display the user missed seeing. However, like humans, automation is never 100% reliable. Automation may fail due to a straightforward malfunction, or it may fail because of an unforeseen situation for which it was not programmed. This has implications for automated systems where the consequences of failure can be dire, such as automated target detection systems which are currently under investigation, or systems which an operate autonomously, such as certain air defense systems. However, there are also implications for how humans interact with automation.

Distrust/over reliance continuum. People's attitudes towards automation reliability, and consequently their confidence in the automation, is somewhat complex. People's confidence in automation is affected by it's reliability. Bowers, Oser, Salas & Cannon-Bowers (1996) pointed out that people's trust in automation follows a continuum from too much trust, which encourages complacency, to too little trust, which discourages people from using the automation. When operators are complacent, they tend not to monitor the operation of the automation sufficiently, so that they are surprised when the automation fails. When they avoid using the automation, they are failing to exploit a possibly advantageous tool. On the other hand, sometimes when people have automated systems to assist them, they can become complacent and allow the automation to perform the task without sufficient supervision (Parasuraman, Molloy, & Singh, 1993). Their vigilance for the task tends to decrease. While this may not be a problem as long as the automation is correctly performing the task, it can be a serious challenge if the automation were to malfunction. Finding the right balance between caution and trust for a particular system can sometimes be quite challenging.

Muir (1994) and Muir and Moray (1996), found that people tend to trust automation the same way they would trust people, in that they place more trust in entities that are predictable and dependable. Lee and Moray (1994) and Eidelkind and Papantonopoulos, (1997) found that people's confidence in the automation dropped dramatically once they experienced a failure of the system. Following this drop their confidence returned slowly, provided the automation performed correctly, but was never as high as before the failure.

Automation failure and failure recovery. An important issue to consider is how automation failure, or the possibility of failure, affects the human-automation interaction. Although systems are most often designed based on perfect performance, in fact all systems

perform incorrectly some percentage of time. The potential for malfunction affects how people interact with automated systems in a number of ways. The most obvious is that when a system fails, the operator must scramble to switch to manual operation in order to continue to perform necessary tasks. If the operator is not aware of how much of the task has been performed by the automation (known as the "out of the loop" problem [McClumpha, James, Green & Belyavin, 1991]), there may be a significant disruption in task performance while the operator attempts to complete the task manually. While this may be tricky during normal operations, it becomes particularly difficult when things aren't going well (Sarter, 1996).

For example, some Tactical Operations Centers (TOC), use an electronic map display which shows the movements of ground forces in near real time. If the TOC happens to lose the display due to a malfunction, there would have to be considerable effort expended to create the same information picture on a common map board. There would also be a disruption in operations while the map board is updated and unit positions verified. If the disruption occurred at the wrong time, it could severely impact the ongoing operation.

Another problem with automation failure is the system may fail without the operator being aware of the malfunction. People typically consider automation to be highly reliable, and are often surprised when it fails (Sarter & Woods, 1997). This may cause them to fail to monitor the automation sufficiently. In addition, when there is a discrepancy between themselves and the automation, people often assume the automation is correct, a phenomenon known as "automation bias" (Mosier, Skitka, Heers & Burdick, 1998).

Automation bias can be a potential problem for an automated system designed to aid the operator in distinguishing between friendly and enemy targets. Normally, the automation would present a classification which would be verified by the operator. However, an operator who experiences automation bias may not sufficiently monitor the automation and may not catch mis-categorizations, allowing friendly forces to be classified as enemy and enemy as friendly. Such mistaken classification can get friendly forces fired upon by other friendlies, while enemy forces can operate without hindrance.

Automation control tradeoffs. Although systems can be set to run autonomously, when safety is a concern the final decision should be made by a human. Billings (1997) listed an automation control hierarchy which described how people and automation can share control of a system (see Table 1). The highest level is fully autonomous operation, where there is no input

by the human, and the lowest level is direct manual control, where there is no input by the automation. In between these extremes are various levels of shared control.

Table 1. *Automation Control Hierarchy (Billings, 1997)*

- Autonomous operation
- Management by exception
- Management by consent
- Management by delegation
- Shared control
- Assisted manual control
- Direct manual control

Automated Aiding of Combat Identification and Fratricide Avoidance: Recommendations

The use of automated systems on the battlefield provides an opportunity to use this automation to aid combat identification and thus reduce fratricide incidents. Automation is used in commercial aviation to aid human performance and reduce aircraft accidents (Wiener & Nagel, 1988, p. 445). In the same way, automation can be used to reduce fratricide incidents. However, given some of the unintended consequences of automation experienced in other domains, it will be important to carefully design the automated aids so that they help reduce fratricide incidents and do not add to the user's task complexity.

Active Versus Passive Automation

One of the considerations for automated aids for fratricide avoidance is whether the automation should be passive or active. Used in this context, passive automation would present timely information to the user that is pertinent to avoiding fratricide, but would require no action from the user. On the other hand, active fratricide avoidance automation would present information to the user and require the user to take action to acknowledge the information. There are advantages and disadvantages to each type of automation, however, because of the criticality of fratricide avoidance, we believe active measures have more advantages than disadvantages in most, though not all, situations.

The primary reason for suggesting active alerts over passive alerting is that the same situations where alerts would be beneficial, such as high stress environments, the user could miss

important information through attentional narrowing and change blindness. Attentional narrowing, the focusing on a central task at the expense of peripheral information, tends to be more prevalent in stressful situations (Wickens, 1992, p. 417). Coupled with what we know about change blindness, we could theorize that, in many military situations where fratricide is a possibility, a user could easily miss important information displayed by the automated system if it was presented passively. There is a greater chance of directing the user's attention to fratricide related information if the user is obliged to take some action in response to the information, such as pressing a button to acknowledge it.

For example, an alert notifying the operator that a new friendly unit has joined the network is less critical than an alert saying a friendly unit has been selected for targeting. For the new friendly unit alert, a simple notice on the display that requires no action by the operator would suffice. However, targeting a friendly unit has dire enough consequences that the automation should doubly ensure the operator is aware of their actions. One method of ensuring the operator's active participation would be to constrain the operator from targeting a unit classified as friendly. Because there is the possibility of mis-classifying the unit by the automation, the operator should be allowed to override the constraint if the operator determined the unit is indeed an enemy. The operator's actions to override the constraint imposed by the automation would ensure the operator was actively involved in the process and reduce the chance that the operator would act unwittingly.

Besides active versus passive automation, there are a number of other considerations to developing a usable automated fratricide avoidance aid.

Other Considerations

Reduce intrusiveness. There are some cautions to using active alerts. In some cases, forcing the user to acknowledge alerts can actually interfere with correcting the problem the alert is warning about. In a high stress and workload environment, interrupting the user's work flow by forcing them to attend to an alert can lengthen the time it takes to correct the problem. In extreme cases, where multiple alerts are competing for the user's attention, they can further hinder the user from correcting the problem (Wickens, Gordon & Liu, 1998, p. 506).

Systems can be designed such that the alerts do not become overly intrusive. In one experiment, Ross, Barnett & Meliza (2007) had participants monitor a simulation of a network-enabled C2 system which had an automated alerting system to notify the operator of various

events that might be fratricide related. They compared the participant's SA and workload with the alerting system enabled and disabled. They found whether the alerting systems was enabled or not had no significant effect on SA, but self-reported workload was significantly lower with the system enabled.

Automation should be adaptable. Even though an active alerting system might be preferable, it should also be carefully designed so that it does not become overly intrusive. One means to do this is to allow users to modify the level of interaction required by the automated aid to be able to adapt to changes in the environment and user priorities. Although requiring the user to acknowledge important information presented by the aid ensures that user is aware of it, the user should be able to quickly and simply modify when the interaction is required and when it is not. For example, the user could push a "don't bother me" switch to set the alerts from active to passive for a set period of time so that he or she could finish a task without interruption. After the set period of time, the aid would automatically revert to the active state. The time limit is to prevent the user from forgetting to change back to the active state and consequently missing important information.

Automation's actions should be visible. The automation should keep the user informed about what it's doing and it's "health" status in a non-intrusive way. Failures should not be silent or hidden. This is important not only as a means for the user to estimate the automation's reliability, but also to help the user revert to manual operation should the automation malfunction. For example, a simple display that shows the current state of the automation, possibly in symbolic form, would be most helpful to the user and would keep the user in the loop. For example, a "stoplight" display that shows either green (proper operation), yellow (partial malfunction), or red (inoperative) would provide status information in a way that doesn't overburden the user's mental workload.

The human operator should be in charge. Since the human operator will ultimately be held accountable for safety and fratricide incidents, the human must be given ultimate authority over the automation. Thus, the highest acceptable level of automation in the automation control hierarchy shown above should be "management by exception," where the system works autonomously unless the operator overrides it. The operator must also be able to easily monitor the automation to be able to override it if required, another reason why automation's actions should be visible. This means the operator must have access to sufficient information, such as

the state of the automation, to be able to make an informed decision quickly, and the automation should provide as much aid to the operator as necessary for the operator to make a correct decision. When necessary, the operator must be able to override the automation easily and quickly.

As an example of why this is necessary, suppose an armored vehicle had a fratricide avoidance system which prevented the crew from firing on another vehicle assessed as friendly. A situation could arise where the automation erroneously determined a vehicle as friendly, when actually it was an enemy preparing to fire on the friendly vehicle. Under fully autonomous operation, if the system prevented the crew from targeting the enemy vehicle (erroneously determined to be friendly), the crew would be unable to fire on the enemy, who would be fully capable of firing on them. Thus the automation, rather than increasing safety, would put the crew in danger with no way of recovering.

Alternately, a system which automatically targeted and fired on vehicles determined to be enemy, or one with an active protection system like those currently under development, could commit fratricide if it erroneously classified a friendly unit as enemy. Again, under full autonomy the human operators would have no way of preventing fratricide.

Automation's usability should be verified. Systems are always designed to work flawlessly, but there are often extraneous variables that creep in when the system is fielded causing unintended consequences. Some users may not employ the systems the way the designers had intended. The environment the system was designed to operate in may be different, or it may change periodically, or it may be more complex than originally envisioned. All of these factors may cause the system to operate other than it was intended.

The way to verify that the system will operate correctly in the field is to test it, either in the field or under realistic field conditions, including using operators that accurately represent the population expected to operate the system in the field. Such user testing is one of the cornerstones of good human-automation interaction, but often time or budgetary constraints minimize or eliminate this vital step in systems design. Given the consequences of failure of the human-automation system to avoid fratricide are dire, thorough user testing is very important in this area.

Conclusion

Automation has the potential to be a valuable aid to fratricide avoidance. Automated alerts could be designed to actively engage operators in fratricide avoidance. However, research has shown that there are a number of issues dealing with automation that must be addressed to ensure automation is a benefit and not a hindrance. There must be an understanding of how automation affects SA, team interaction, and decision making. There must also be an understanding of how humans work with automation, in particular how this is different from how people work with other people, as well as considerations about how people deal with automation failure. While some of these concerns can be complex, with a good understanding of the issues, along with careful design and testing, automated systems can be developed which will work with the operator to reduce the probability of fratricide to its lowest level.

References

Billings, C. E. (1997). *Aviation automation: The search for a human-centered approach*. Mahwah, NJ: Lawrence Erlbaum.

Bowers, C. A., Oser, R. L., Salas, E. & Cannon-Bowers, J. A. (1996). Team performance in automated systems. In R. Parasuraman and M. Mouloua (Eds.) *Automation and human performance: Theory and applications*. Mahwah, NJ: Lawrence Erlbaum Associates.

Durlach, P. J. (2004) Change blindness and its implications for complex monitoring and control systems design and operator training. *Human-Computer Interaction 19*, pp. 423-451.

Durlach, P. J. & Chen, J. Y. C. (2003). Visual change detection in digital military displays. *2003 Proceedings of the Interservice/Industry Training, Simulation, and Education Conference* (I/ITSEC). Arlington, VA: National Training Systems Association.

Durlach, P. J., Kring, J. P. & Bowens, L. D. (in press). Detection of icon appearance and disappearance on a digital situation awareness display. *Military Psychology*.

Eidelkind, M. A. & Papantonopoulos, S. A. (1997). Operator trust and task delegation: Strategies in semi-autonomous agent system. In M. Mouloua and J. M. Koonce (Eds.) *Human Automation Interaction: Research and Practice.* Mahwah, NJ: Lawrence Erlbaum.

Endsley, M. R. (1988). Situation awareness global assessment technique (SAGAT). *Proceedings of the National Aerospace and Electronics Conference (NAECON)*, 789-795. New York: IEEE.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors 37*(1), 32-64.

Endsley, M. R. (2000). Theoretical underpinnings of situation awareness: A critical review. In M. R. Endsley & D. J. Garland (Eds.), *Situation awareness analysis and measurement*. Mahwah, NJ: LEA.

Gugerty, L. J. (1997). Situation awareness during driving: Explicit and implicit knowledge in dynamic spatial memory. *Journal of Experimental Psychology: Applied 3* (1), 42-66.

Jones, D. G. & Endsley, M. R. (1996). Sources of situation awareness errors in aviation. *Aviation, Space, and Environmental Medicine 67* (6), 507-512.

Lee, J. D. & Moray, N. (1994). Trust, self-confidence and operators' adaptation to automation. *International Journal of Human-Computer Studies 40*, 153-184.

McClumpha, A. J., James, M., Green, R. G. & Belyavin, A. J. (1991). Pilot's attitudes to cockpit automation. *Proceedings of the Human Factors Society 35th Annual Meeting.* Santa Monica, CA: The Human Factors Society.

Mosier, K. L., Heers, S., Skitka, L. J. & Burdick, M. (1997). Patterns in the use of cockpit automation. In M. Mouloua and J. Koonce, *Human-Automation Interaction: Theory and Applications*. Mahwah, NJ: Lawrence Erlbaum Associates.

Mosier, K. L., Skitka, L. J., Heers, S. & Burdick, M. (1998). Automation bias: Decision making and performance in high-tech cockpits. *International Journal of Aviation Psychology 8*(1), 47-63.

Muir, B. M. (1994). Trust in automation: Part I. Theoretical issues in the study of trust and human intervention in automated systems. *Ergonomics 37*(11), 1905-1922.

Muir, B. M & Moray, N. (1996). Trust in automation. Part II. Experimental studies of trust and human intervention in a process control simulation. *Ergonomics 39*(3), 429-460.

Parasuraman, R., Molloy, R. & Singh, I. L. (1993). Performance consequences of automation-induced "complacency." *International Journal of Aviation Psychology 3*(1), 1-23.

Ross, J. M., Barnett, J. S. & Meliza, L. L. (2007). *Effect of audio-visual alerts on situation awareness and workload in a net-centric warfare scenario*. Poster presented at the 51st annual meeting of the Human Factors and Ergonomics Society, Baltimore, Maryland, October 1-5, 2007.

Sarter, N. B. (1996). Cockpit automation: From quantity to quality, from individual pilots to multiple agents. In R. Parasuraman and M. Mouloua (Eds.) *Automation and human performance: Theory and applications*. Mahwah, NJ: Lawrence Erlbaum Associates.

Sarter, N. B. & Woods, D. D. (1997). Team play with a powerful and independent agent: Operational experiences and automation surprises on the Airbus A-320. *Human Factors 39*(4), 553-569.

Shrader, C. R. (1982). *Amicicide: The problem of friendly fire in modern war*. Fort Leavenworth, KS: Combat Studies Institute.

Wickens, C. D. (1992). *Engineering psychology and human performance* (2nd Ed.). New York: HarperCollins.

Wickens, C. D., Gordon, S. E. & Liu, Y. (1998). *An introduction to human factors engineering*. New York: Longman.

Wiener, E. L. & Nagel D. C. (1988). *Human factors in aviation*. San Diego, CA: Academic Press.