Next Generation Air Transportation Systems: Human-Automation Interaction and Organizational Risks

Thomas B. Sheridan
Volpe National Transportation Systems Center, U.S. Department of Transportation
Cambridge, MA 02142 USA
<Sheridan@volpe.dot.gov>

Abstract. Both the US and European Community are now undertaking major projects to double air traffic capacity. It is believed that this will demand a significant increase in automation and a redefinition of the human air traffic controller's role to be that of a supervisor of the automation and an intelligent agent to make tactical decisions in off-normal situations. This paper discusses the associated issues of the envisioned human-automation interaction and the concomitant organizational complexity, primarily from a US perspective. It also suggests the envisioned approach to considering risks and designing a resilient human-machine system.

1. BACKGROUND

Air traffic demand is predicted to double by 2020-2025 in the U.S., Europe, China and elsewhere. The larger airports in the U.S. and Europe are currently operating at full capacity. Economic and construction delay and cost factors suggest that mostly the same airports and runways will have to be used, and especially smaller airports used more efficiently to supplement the larger airports. Radar surveillance technology has been shown to err by up to 1/2 mile, depending on aircraft distance from a radar site. (This constraint is largely responsible for regulations that restrict aircraft separation to 5 miles horizontal and 1000 feet vertical in enroute airspace, and 3 miles, 1000 feet in airspace near airports.) Behavioral analysis indicates that human air traffic controllers cannot observe and vector many more aircraft than they now handle in a sector. And it is far from clear that just adding more controllers would be affordable, or would even work in any case. Since personnel constitute the greatest cost factor, the hope would be to keep the number of personnel the same or

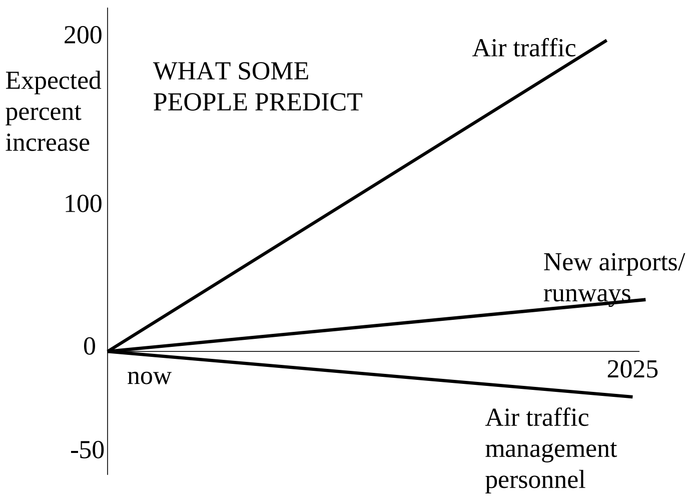


Figure 1. Assumptions underlying planning for the Next Generation Air Transportation System

actually decrease the number. For all these reasons it has been decided that a radical departure from the current, mostly manual, air traffic control system must be put in place. Figure 1 shows the trends that underlie this decision.

In the U.S. an inter-agency Joint Planning and Development Office (JPDO) for the Next Generation Air Transportation System (NGATS) was set up in 2004. In addition to its own planning staff are eight Integrated Project Teams (IPTs) responsible respectively for: agile air traffic management; airport infrastructure; proactive safety management; user-specific situation awareness (including a new broadband information network); weather observation, prediction and impacts; security (presumably without limiting mobility or civil liberties); harmonization of equipage and operations globally; and environmental protection (with sustained economic growth). Each IPT has representatives from various government agencies, principally the Federal Aviation Administration (FAA), the agency responsible for aircraft certification, air traffic control as well as training of control personnel, and the National Aeronautics and Space Administration (NASA), the agency that has been primarily responsible for aviation research and development. Because global positioning satellite (GPS) technology will play a key role in the new system the US Department of Defense (that is responsible for those systems) is also a player, as are the Environmental Protection Agency (EPA), the Department of Commerce, and the Department of Homeland Security (DHS), all included for obvious reasons. In addition an organization called the NGATS Institute has been set up to include industry participants and perspectives. The organizational complexity of the project is evident.

The European Community has a similar, if less complex, organizational structure (SESAR project) for planning a next-generation air transport system.

2. THE VISION

Based on nominal schedules, weather observation and prediction (that are assumed to be much better than now), fuel considerations (that are expected to be more critical than now), and improved Global Positioning System (GPS)-enabled Automatic Dependent Surveillance-Broadcast (ADS-B) surveillance technology, a large-scale computer system would determine and negotiate with flight crews, airline operations managers and air traffic managers for (near) optimal 4D trajectories (3 in space, one in time). This would be for all phases of flight (climb, cruise, descent and taxi) for participating flights and aircraft that are properly equipped. Non-equipped aircraft would be restricted to lower altitudes and be otherwise constrained. Participating aircraft would be controlled in flight mostly automatically, with guidance coming from the external air traffic management computer system. Operations on airport surfaces would be planned correspondingly and controlled mostly by computer. The roles of both flight crew and air traffic management personnel would change significantly in the direction of their becoming monitors of automation, presumably intervening when anomalies or emergencies occur that the automation cannot resolve. Much more information would be available to flight crews and ATM personnel over a broadband communication network, where communication would mostly be mediated by digital "data-link." Further information on such planning is available in JPDO (2005), ICAO (2005), and FAA (2006).

3. ISSUES OF HUMAN-AUTOMATION INTERACTION

This US JPDO vision for the future, which is mostly shared by the European SESAR project, poses many challenges and risks in relation to the interaction between the humans and the automation in the system (Sheridan and Corker, 2006; Sheridan, 2006; Parasuraman et al, 2000), both with respect to the operational functions and with respect to the organization and management of the system. Among these challenges and risks are:

a. Confusion over who (human) or what (computer) has authority at different stages of flight. This includes possible misunderstandings in negotiations over the 4D trajectories enroute and 3D trajectories on airport surfaces. It includes issues of what happens when an aircraft deviates from the agreed upon trajectory, either for lack of attention by the flight crew or air traffic controllers who are supposed to be monitoring, or because of weather, or in medical/security emergencies.

b. Misunderstandings regarding what network information would be "pushed" (manditorily displayed to human operators), what would need to be "pulled" (explicitly requested), and what would be restricted and to whom. This includes all the issues of delays and confusion in using data-link rather than the more intuitive voice communication medium.

c. Problems of robustness, reliability and operator trust in computer-based decision support tools and computer control in general. Because of the greater interconnectedness of aircraft and subsystems, equipment failures and misapplied procedures can cause perturbations that cascade throughout the whole system.

d. Control instabilities resulting from closed-loop time delays due to air traffic controller time-sharing of attention, or needed perceptual and decision time. These may be a result of poor designs that presume continuous control of aircraft by the ATM system and do not properly account for unexpected time delays for humans to receive and comprehend complex patterns of information and make proper decisions.

e. Operator error in mental modeling of the automation and in situation awareness of what the automation has done, is doing, or can be expected to do. Current selection and training of air traffic controllers places little emphasis on understanding and use of computer automation, and is mostly directed toward training the perceptual-motor skills of vectoring individual aircraft. The new system will require a different emphasis.

f. Lack of a "safety culture" that encourages operator recognition and reporting of errors and near-miss situations. The current air traffic management system is designed to measure controller and pilot errors seemingly for the purpose of reprimanding and punishing, and it is no surprise that many or even most runway incursions and airborne aircraft separation violations currently go unreported.

g. Design errors in assuming simple linear scalability of engineered systems as the transition is made from the current to the new technology and to more aircraft flying with closer separations.

The above are only a sampling of the human-automation challenges and risks posed by NGATS planning.

4. ACHIEVING A RESILIENT SYSTEM

While the issues recited above are certainly neither new nor unique, the magnitude of the NGATS developments in terms of technological complexity and cost make it imperative that the best current thinking be applied to make NGATS resilient to unexpected circumstances. A major accident in the early stages of NGATS implementation can halt progress and bring the whole air transportation system to a standstill while remedial efforts are made.

A look back at a sample of 38 accidents and system failures traceable to human-automation interaction (20 in aviation, 6 with other vehicles, 5 in process control and 7 in other systems) revealed that judged "reasons" for failures were relatively evenly divided between system design, management (or operation and maintenance), training of operators, and improper or ineffective procedures (Sheridan, 2006). In about half the cases failure was clearly a combination of these factors.

Surely any large project should exploit all or most of the standard tools of risk analysis as they are deemed applicable: fault trees, event trees, and other systematic means of considering safety such as the SHARP (Moieni, et al., 1994) and ATHEANA (NUREG-1624, 2000) approaches used by the US Nuclear Regulatory Commission to identify vulnerabilities of human-technology interaction.

It is expected that the primary way to ensure safety is by proactive efforts to make systems resilient (Hollnagel et al., 2006). Such efforts should include detailed task analysis, extensive human-in-the-loop simulation and fast-time computer simulation where feasible, and cost-effective decisions about instrumentation and research to provide needed and timely information.

Abstract Task Analysis First, Then Function Allocation and Risk Analysis

Every human factors engineer knows about task analysis, and it is easy to assert that every redesign of a system should begin with task analysis. The general image of performing a task analysis is that of observing operators doing the task in the current system and noting what they observe and what actions they take. Cognitive task analysis, which is becoming quite popular, goes a bit deeper. Through not only observations but also interviews, focus groups, etc. it tries to infer what must be remembered and what decisions must be made by operators.

However such observation and operator interview techniques fall short when the vision is of a system radically different from the present one, and when it involves a large increase of automation hoped to work closely in cooperation with human operators. In that case it is important to step back, use a "blank piece of paper," and, at each stage of the envisioned process, identify which *physical variables* must be measured how often and to what accuracy, what decisions must be made in terms of those variables, and what physical variables must be controlled with what bandwidth and what accuracy. In such an approach the task is conceived in the abstract, and no decision is implied about whether measurements, decisions or control are executed by a human or by a machine.

Only after such an abstract task analysis is in hand should the function allocation of whom or which (human or computer) does what and when be decided. The risk analysis then goes hand in hand with the function allocation, for at this point one can decide whether the human or machine can perform to standard with adequate reliability, or if the workload of that task or some other (concurrent) task is too high, or if human or machine can better accomplish situation awareness, and so on (Sheridan, 2000).

Human-In-the-Loop and Fast Time Simulation Iterated at Multiple Stages of Development

Human-in-the-loop (HITL) simulation is a well-known and obvious need for any large system development involving people and technology interacting. The business case for HITL has been established (Krois and Rehmann, 2005). Traditionally, however, HITL simulations have been regarded as very expensive, because they (have been seen to) require relatively full-scale hardware and software setups that have face validity but are quite expensive to construct and operate. Hence managers have been loathe to utilize HITL until systems are relatively well developed (and substantive changes are discouraged). This is very wrongheaded, since much can be learned from relatively crude HITL simulations, at least with respect to human-automation interactions. Such simulations should be done early in development to provide early warnings of problems to be faced and further researched. The results of these activities should be accommodated in refined designs, and the simulations should be iterated as development proceeds.

If sufficiently good models of system processes and human observation, decision and response are available, then fast-time computer simulation is also an option, and is normally much cheaper than HITL simulation. However the literature supports relatively few areas amenable to quantitative dynamic models of human performance. Among these are visual and auditory signal detection, continuous control, statistical decision-making, and information processing (Sheridan, 2002). One particular issue that arises in NGATS is the fact that human decisions take time, and when humans are called upon to evaluate complex situations that are unexpected and off-normal the response time may be quite long. It is well known that the distribution of human response times is highly skewed to the right (Figure 2) and in fact fits a log normal model quite well. For example, in one study of roughly one hundred nuclear power plant operator teams responding to a large-break loss-of-coolant-accident (LOCA), while the median response time was only 20 seconds the 95th percentile response time was over 100 seconds (Kozinsky et al., 1982).

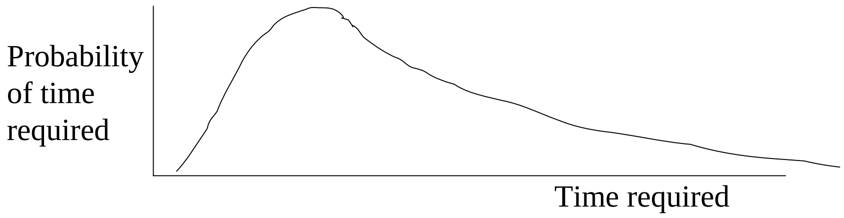


Figure 2. Highly skewed human response time for complex observations/decisions

This fact is relevant to NGATS in the following way. Longitudinal control of an aircraft must be maintained to ensure proper separation from other aircraft. Such control is achieved by a series of nested control loops, such as shown in Figure 3, where the flight management system (FMS) controls the aircraft, the pilot controls the flight management system, the air traffic controller controls the pilot, the ATC supervisor controls the controller, the regional center traffic management unit (TMU) controls the supervisor, and a single flow control command center (at least in the U.S.) in conjunction with each airline's operation center (AOC) controls the whole national system. Except for the FMS-aircraft loop, the other loops operate intermittently, and the higher in the structure the control agent is, the less frequent the control action. However, NGATS plans are considering more automation for some of these loops (not yet determined), and one concern is that time delays in the outer control loops can produce instability.

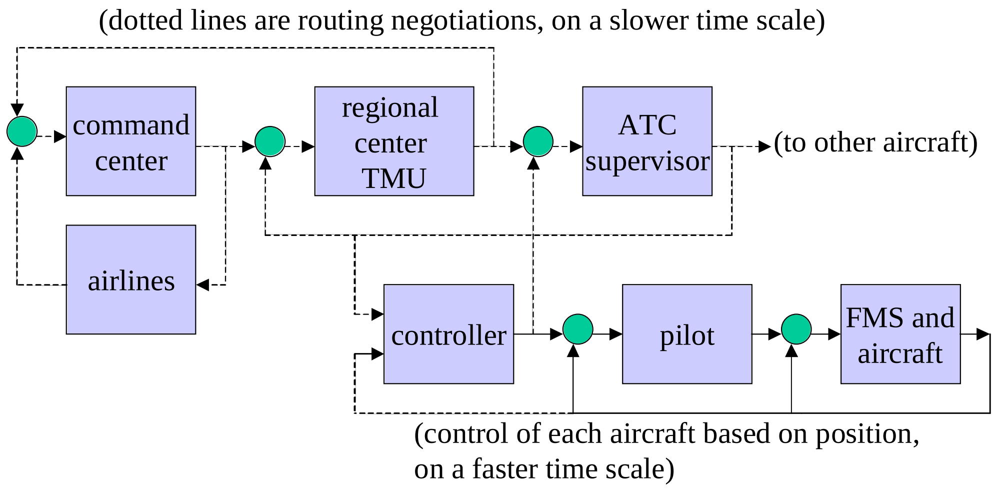
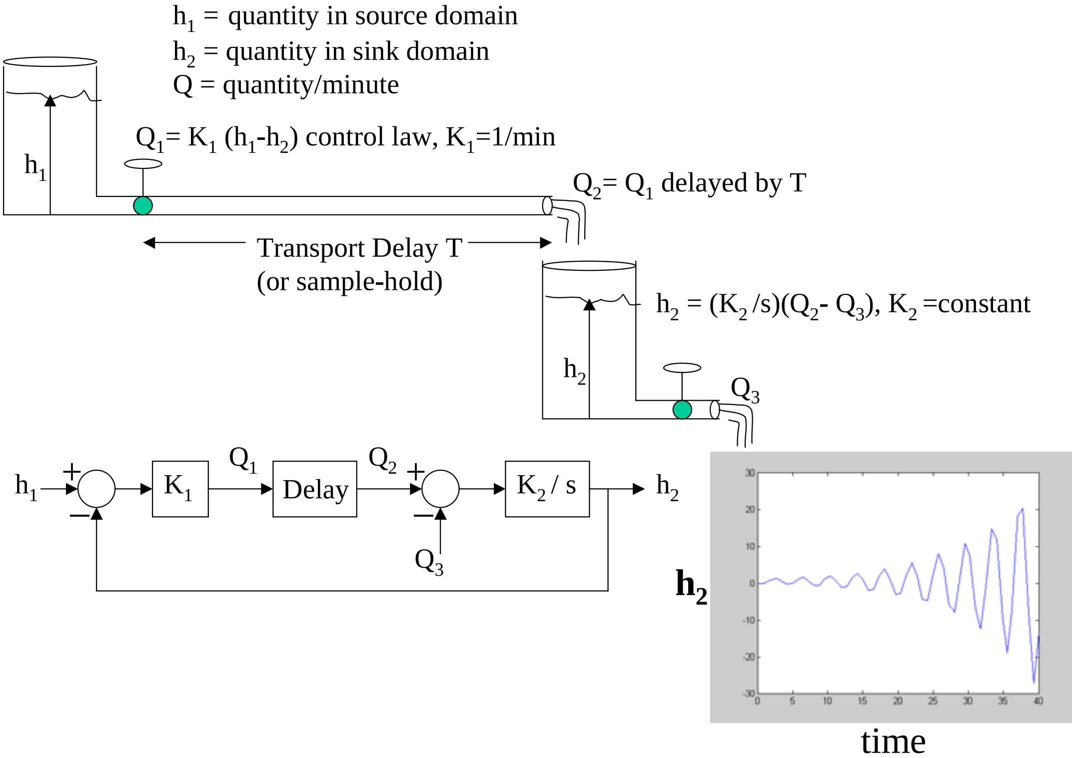


Figure 3. Air traffic management as a control system with multiple nested loops

Simulation experiments (Sheridan et al, 2006) have demonstrated this effect, well known to control engineers. Figure 4, using the metaphor of liquid (or aircraft) "flowing" from one "tank" (sector of airspace) to another, and quantity in the second tank (aircraft within another sector of airspace or on the airport surface) being controlled as a function of the difference between source and sink levels of liquid in the tanks (traffic in the sector). There is necessarily a delay between the time a given aircraft is observed upstream and when that same aircraft is observed downstream, and so regulating the speed ("flow") for the aircraft upstream amounts to a delay in the control loop, as shown in the lower diagram of the figure.

If such control is executed continuously in time an instability results, as shown in the plot. The same is true for a decision delay produced in an outer-flow control loop of Figure 3.



.

Figure 4. Upstream control of aircraft to maintain spacing from downstream traffic. Flow cascade between tanks analogy (upper figure). Block diagram with delay element (lower left). Plot of unstable response (lower right).

Information Value

An under-appreciated factor in human-machine safety is what has been referred to as *information value*, which bears on the salient issue of the cost of safety (Howard, 1966; Sheridan, 1995). Providing information, whether through aircraft or ground-based instrumentation, or by performing research, costs money and time. Information value is the difference between the outcome of an event when sufficient information is available to take the control actions best suited to each occurring situation (state), and the outcome when such information is not available (and therefore control actions can be taken only on the basis of the expectation (probability of various situations). The difference is illustrated by a simple example as shown in Table 1.

Table 1. Simple two-situation example of information value calculation. The table shows the probability of each of two possible situations and the contingent worths when alternative actions are taken with full knowledge of those situations. At the bottom are expected worths when only the situation probabilities are known.

	Probability	**Action x**	**Action y**
Situation X	0.95	Worth = 0	Worth = -10
Situation Y	0.05	Worth = -100	Worth = 0
Expected Worth		EW = -5.0	EW= -9.5

Suppose only two possible situations (states of the world) can occur, X or Y, and their known probabilities are as shown in the table. Suppose x and y are the appropriate responses for X and Y respectively, such that taking these correct contingent actions nets zero worth, while taking incorrect actions nets negative worth outcomes (or costs) as shown. If information as to the true situation is lacking the best a decision-maker can do is take that action with the greatest expected worth (or if highly risk averse take some other single action) no matter what the truth of the situation. There is an obvious difference in outcome, and this difference is called the information value. In general there will be many (or even a continuum) of possible situations and possible actions, so that instead of a simple 2x2 table we could have a large matrix of outcome worths or a two-dimensional plot, but the same idea would apply. Thus information value is the difference between the first two terms for expected outcome worth (W) in the following equations (worth numbers can designate benefit or cost). Now also consider that that gaining any information usually has some cost C, so that the net worth is the information value minus the cost of that information:

Net worth = (expected worth for perfect information) - (expected worth for no information) - cost of getting the information) = 0 - 5.0 - C

For a multiplicity of situations and alternative actions the general formula is

$$W_{(net)} = \Sigma_i\ P(S_i) \text{ max over } A_j \text{ of } [W(S_iA_j)] - \text{max over } A_j \text{ of } [\Sigma_i P(S_i)\ W(S_iA_j)] - C$$

Thus, for any instrumentation being considered, insofar as a system designer can estimate probabilities for a set of situations that might be encountered as well the relative worths (or costs) of the outcomes contingent on alternative actions that might be taken, one can determine the information value. And if the cost of acquiring the information is known one can assess whether it is worth providing the instrumentation. The same thinking can be applied to any investigation, where the anticipated results are assumed to indicate the best action for each situation, and where otherwise a decision-maker is left guessing about what is the best policy. Obviously actions appropriate to the occurring situations not only cost less but also are safer.

5. ORGANIZATIONAL ISSUES (U.S.)

Up to now in the U.S., NASA has performed aviation research at multiple levels, ranging from basic science (e,g., fluid dynamics, combustion, electronics, and human cognition) to highly applied system design (e,g., design of sensors, flight deck displays, controller decision support tools). Often long-term projects have been carried through from the former to the latter, resulting in subsystems that could be handed off to FAA for final validation tests and certification. This approach has worked rather well, and the aviation industry has appreciated NASA's contributions.

Current policy, motivated by tight government budgets and competition within NASA for space projects directed toward a manned Mars mission, is that NASA will not engage in system development and should concentrate on the more fundamental research (with a smaller budget), and industry should perform the system development in conjunction with FAA.

However there are considerations that might lead one to question the current policy: (a) NASA is already staffed with the requisite engineering talent and test facilities which would have to paid for anyway if industry were to pick up the development; (b) FAA does not itself have the engineering manpower or budget to do engineering development or even to coordinate and monitor system development by industry; and (c) JPDO is a planning and envisioning organization without staff to do research and development. Hence a gap is emerging between the more fundamental research that NASA, together with universities, is now being paid to do, and FAA and JPDO, which are not equipped to handle the all-important transition from research to system design and development prior to final testing and certification by FAA. Morale within NASA at this writing is being affected. This is bound to impinge on the comprehensiveness of safety considerations that go into the system design.

If the rather ambitious U.S. plan for NGATS is to be realized and safe, the transition from research to development to design to validation/verification should best be continuous and overseen by a single responsible agency. The NASA Apollo (lunar landing and exploration) project is often cited as an exemplar. Apollo had a tight and unified government chain of command that involved many private contractors in the actual design and construction.

6. CONCLUSION

Plans for the next generation of air transportation systems call for a radical departure from current systems with respect to human-automation roles and interaction. This paper discusses several issues that must be dealt with to ensure safety and system resilience.

ACKNOWLEDGEMENT

This work was supported by the Airspace Systems Program of the National Aeronautics and Space Administration, USA.

REFERENCES

FAA (2006). *Roadmap for Performance-Based Navigation.* Washington, DC.

Hollnagel, E., Woods, D.D and Leveson, N.(2006). *Resilience Engineering*. Burlington, VT: Ashgate.

Howard, R.A. (1966). Information value theory. *IEEE Trans. on Systems Science and Cybernetics.* SSC-2, 22-26.

ICAO (2005). *Global Air Traffic Management Operational Concept, First Edition*, Document 9854. Montreal, Quebec.

JPDO (2005). *Progress report on the Next Generation Air Transportation System Integrated Plan*. Washington, DC.

Kozinsky, E., Pack, R., Sheridan, T., Vruels, D. and Seminara, J. (1982*). Performance Measurement System for Training Simulators*. Atlanta, GA: Electric Power Research Institute Report NP-2719.

Krois, P. and Rehmann, J. (2005). *Assessing Human Factors Risks in Air Traffic Management Research.* Washington, DC: DoT/FAA Technical Note AR-05/1.

Moieni, P., Spurgin, A.J. and Singh, A. (1994). Advances in human reliability analysis. Part I: frameworks, models and data. *Reliability Engineering and System Safety* 44, 27-55.

NUREG 1624 (2000). *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA).* Washington, DC: U.S. Nuclear Regulatory Commission.

Parasuraman, R., Sheridan, T.B. and Wickens, C.D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems Man and Cybernetics*, SMC 30(3), 286-297.

Sheridan, T.B. (1995). Reflections on information and information value. *IEEE Trans. on Systems, Man and Cybernetics*, SMC-25(1), 194-196.

Sheridan, T.B. (2000). Function allocation: algorithm, alchemy or apostasy? *International Journal of Human-Computer Studies*, 52, 203-216.

Sheridan, T. B. (2002). *Humans and Automation*. New York, NY: Wiley.

Sheridan, T.B. (2006). *A Review of Human-Automation Interaction Failures and Lessons Learned*. Cambridge, MA: Volpe National Transportation Systems Center.

Sheridan, T.B., Bürki-Cohen, J., and Corker, K. (2006). Human transient into-the-loop simulation for NGATS. *Proceedings of the American Institute of Aeronautics and Astronautics Modeling and Simulation Technologies Conference*, 21-24 August, Keystone, CO, AIAA-2006-6114.

Sheridan, T. and Corker, K. (2006). *Report of a Workshop on Human-Automation Interaction in NGATS*, Cambridge, MA: Volpe National Transportation Systems Center.

Sheridan, T.B. and Parasuraman, R. (2006). Human-automation interaction. In R. Nickerson (Ed.), *Reviews of Human Factors and Ergonomics*. Santa Monica: Human Factors and Ergonomics Society.