INL/CON-09-15281
PREPRINT

Human Factors and Data Fusion as Part of Control Systems Resilience

HSI 2009

David I. Gertman

May 2009

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint should not be cited or reproduced without permission of the author. This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the United States Government or the sponsoring agency.

Human Factors and Data Fusion as Part of Control Systems Resilience

David I. Gertman, PhD
†Idaho National Laboratory, Idaho Falls, ID 83415

Abstract —**Human performance and human decision making is counted upon as a crucial aspect of overall system resilience. Advanced control systems have the potential to provide operators and asset owners a wide range of data, deployed at different levels that can be used to support operator situation awareness. However, the sheer amount of data available can make it challenging for operators to assimilate information and respond appropriately. This paper reviews some of the challenges and issues associated with providing operators with actionable state awareness through data fusion and argues for the over arching importance of integrating human factors as part of intelligent control systems design and implementation. Human factors methods are proposed as a means by which to improve system performance, resilience, and safety.**

Keywords — **Cognition, control systems, data fusion, human factors, human reliability, resilience, state awareness.**

I. Introduction

Resilience engineering refers to both a paradigm for safety management as well as a description of system adaptability and ability to recover to a stable state in the face of disturbance, either intentional or unintentional. [1] Variations in this basic definition can be found in recent sources [1-2]. As part of a general resilience framework, human actions and interventions that recover, reestablish or maintain system functions, and or that prevent loss are part of resilience. During incidents conditions are dynamic, equipment may be unavailable, and information for operators regarding system status may be highly uncertain. Human response under these conditions can be challenging. The human may have to detect patterns and trends as events unfold or preemptively to shift strategy in anticipation of changing demands. [3] Data fusion presented in process overviews has evolved as a means by which to assist the operator during such conditions.

Depending upon the contextual elements comprising the situation, facility personnel may interact with one another or with other intelligent agents to make time critical decisions affecting process safety or efficiency. With the increasing availability of digitally based smart instrumentation large amounts of data can be at the finger tips of operators. However depending on how this data is collected, assembled, organized, and fused it can obscure rather than clarify important parameter status information. Somehow this increase in bandwidth must be managed to support resilience by decreasing operator workload rather than shifting it. For example, crews can become preoccupied in solving a problem highlighted by changes in display instrumentation and fail to monitor additional parameter information associated with a second problem. A classic example of this in the aviation industry was NYC-Miami Eastern Flight #401. Thus, fusion needs to match elements of operator cognition and support overall state awareness.

Readily available human factors research in establishing engineering practices, handbooks and studies of human error have labored to establish a technical basis for optimizing human performance in high technology high consequence systems. [4-6] Display design guidance from regulators exists as well. [7] However, much of this work in [7] has been focused on optimizing performance based upon considerations regarding mental and physical limitations where system information was presented to operators in analog fashion i.e., discrete components, physically adjustable, with indicator lights or alarms and alarm lists, where the data stream was manageable, and human in the loop performance is often limited to responding events where system dependencies are well established and understood. This has been true for a wide range of systems. Contrast this with the role of the human monitoring self optimizing control systems where under varying conditions data integrity for system state may be compromised, where recovery actions may not be well enveloped by procedures, and where adaptability including communication with other plant engineering specialties may be the key to successful recovery. The latter situation is one wherein the unknowns are high, adaptability is important and system resiliency is a necessity.

A. *Data fusion.*

Data fusion has evolved as an approach to organizing, interpreting, and presenting an operator with information. The important vision of resilient systems can not be realized without some redirection in human factors thought on the part of technologists, asset owners, and management. Too often, data fusion and abstraction has

Work supported by the U.S. Department of Energy under DOE Idaho Operations Office Contract DE-AC07-05ID14517, performed as part of the Instrumentation, Control, and Intelligent Systems Distinctive Signature (ICIS) of Idaho National Laboratory.

evolved as the product of talented individuals implementing their individual design ideas. We maintain that the exponential growth of smart systems in applications such as process control should be complemented by the appropriate human factors research. This research should address the need for models and data supporting first principles for fused information presentation for diverse critical functions such as process control, cyber and physical security. The appropriate way to develop models, methods, and data is through controlled studies.

Improving critical infrastructure situation awareness is to be attained by identifying end user needs and intelligently combining information from multiple sources to produce a comprehensive composite picture. Today, situational awareness associated with the operation of critical infrastructure processes and facilities including interaction with digital control systems are primarily reactive in nature, rather than strategic and preemptive. Integration of security and process information associated with facilities operations, can enable rapid understanding, facilitate impact assessment and thus, support a vision of more resilient and efficient critical infrastructure facility operations.

B. Notable attributes for resilience.

Woods [2, pp 23] lists some of the attributes notable in monitoring, managing and implementing resilience; buffering capacity (size and kinds of disruptions the system can absorb or adapt to), flexibility (ability to restructure in response to external events or factors), margin (in relation to performance boundaries), and tolerance (how a system behaves near a boundary). For example, does the system degrade gracefully or collapse quickly in the presence of change. What is the human role within each of these features of resilient systems? For example, How can operator decision making support buffering capacity or flexibility? How do we express this quantitatively?

C. Role of the operator.

The human is a key factor in appropriate plant response to off normal events in advanced instrumentation and control (I&C) environments including those events representing malicious attack through physical or cyber means. In order to be effective, operators require a window into the process which supports their situational awareness. Currently, process operations are protected by design practices reflecting diversity, redundancy, safety margin and defense in depth. However, time to mitigate often is a function of the operators understanding of systems dependencies. The task of monitoring process performance during emergency conditions is often information intensive and dynamic. During high stress events, human information processing is often limited and information overload becomes acute. Yet, this is precisely when we want human intervention to be best.

With advances in sensor technology used to monitor process status and take control actions, in cyber security, and physical security systems there is the potential to overload the operator during emergency events. Historically, those events (even in analog systems) with multiple faults, are more complex, may have confusing signatures, require knowledge across disciplines (computer science, security, and process knowledge), are fast paced and can be difficult to diagnose. For certain applications, from food processing to refineries, loss of process control can result in trapping product in columns that may have safety or financial repercussions. Further, technology advances such as precise control algorithms that focus upon diagnosis, prognosis, and pre emptive control actions may be ineffective for plant upset conditions where data stream integrity is under attack, the operator's window on the world has purposefully been made misleading, or there may be little historical basis for response.

D. Capability versus Usability. Many of us know that people will often choose capability over usability. This can be the case in applications that seem to afford the user too much information to the point of distraction. A simple example, is in providing operators with a large display hierarchy where the rules of screen navigation are cumbersome, not well understood and fail to leverage population stereotypes.

II. LEARNING FROM VARIOUS DOMAINS

Since Three Mile Island, human factors involvement in the nuclear industry has been to support safe operations through control room design review, human factors guidelines for the format of procedures, staffing studies, characterization of human performance in operating events and in review of safety critical operator actions as presented in licensee submittals. In the latter application, training principles, human reliability analysis has been used to quantify human failure rates used in probabilistic risk analysis.

In the Department of Defense community, human factors engineering guidelines exist in MIL STDs such as [8]. Ergonomics handbooks, and texts on human computer interaction are also available. Conspicuous in its absence are guidelines for data abstraction and data fusion for high technology operating environments, such as nuclear power plants, chemical processing, grid operations or enrichment facilities. Guidelines that do exist are somewhat nebulous for determining when there is too much information available to decision makers or when the information presented is not useful. Because users differ in their experience and information needs vary as a function of operational state and incident type, usability testing is usually conducted as part of any display design and implementation process. However, it is common that the level of data abstraction presented to operators can vary within similar as well as different facilities and infrastructures. In many cases, operations determine what information needs to be made available, determine what

form the data should take and make decisions regarding fusion and abstraction. Difficulties arise when other data types are introduced.

Since 2001, all US infrastructure has been alerted to the potential for physical or cyber attack from domestic or foreign nation state sources. To what extent confirmatory data regarding these attacks should be presented to operations is open to discussion. Further, in terms of not overwhelming the operator, processed rather than raw data feed is often preferable. Research is required both to determine the appropriate level of abstraction of sensor, process, or cyber security (IDS), or security data to support decision making. The fundamental principles for integration that can be used to guide the next generation of display design are also needed.

Thus, to date there is no individual model of, nor data elucidating first principles for the visualization of fused information that cross cuts process control, cyber security and physical security data. The design of well crafted laboratory and field studies holds promise for determining these principles. Some work has already been done in the development of decision aids employing fusion concepts.

D. Decision aids

Data aids employing fusion concepts have found implementation in military applications. One of the earlier examples of data fusion in support of command and control can be found in Waltz and Llinas [9]. As they state, fusion can be characterized by corresponding levels of information content and uncertainty associated with that content. Data combination and meaning are aspects of fusion. In various military applications, systems users query the system to obtain information on patterns from which to infer threats. It seems reasonable that this use of fusion would hold for non-military applications as well. In robotics fusion and abstraction principles are applied routinely to allow operators to visualize and take control actions through the same interface. For example, in a recent study operator preference was highly positive for fused and abstracted information characterizing a high threat environment [10].

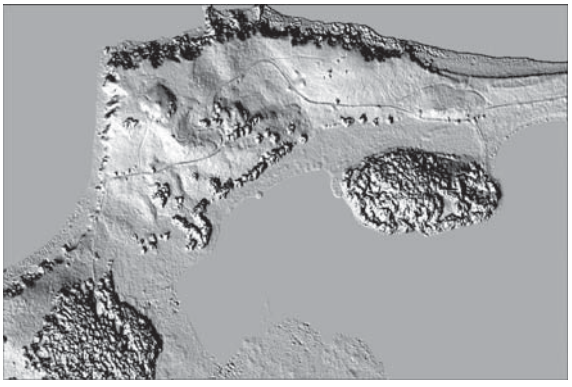
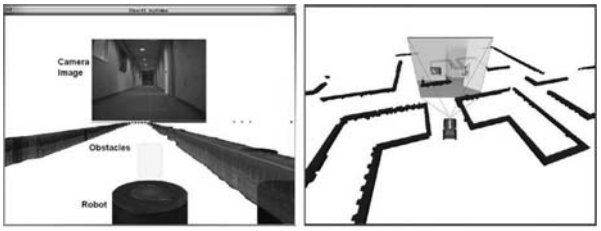


Figure 1 Sensor Example, Shaded relief map – *Source NOAA, Google images 2008*

Figure 1 presents a simple fusion example where a shaded relief map of Kodiak Island has been produced. The image has been produced by merging data from several different sensors. This is representative of pixel level data fusion; other types of fusion include decision level fusion used in military and robotic applications.

In the field of robotics, unmanned ground vehicles and unmanned aerial vehicles have typically been controlled and navigated with an interface that organizes different data sets into multiple windows made available on a single screen. With this approach the user performs the data fusion internally. [11] This is to be contrasted in applications where situation awareness and performance have been enhanced by performing this fusion for the user and presenting a fused characterization of the environment on a single display interface. In [11] the researchers apply ecological design based on Gibson's theory of affordances to create a 3D virtual environment augmented with real time video, map and robot pose information. In figure 2, the robot size has been scaled to the environment and the user can adjust the perspective.



(a) (b)

Figure 2. Fusion paradigm comparing raw range data (a) with integrated fused display (b) – ref 11

Within this environment users are able to navigate in less time and with fewer collisions than when using a 2D interface with multiple windows. The authors' analysis concluded that fusion-based displays should allow for user- adjustable perspective and provide a common reference frame to help guide user actions. The primary challenges lies in adapting the interface to meet the mission objectives of the individual end user.

III. HUMAN FACTORS APPROACHES

Human factors approaches to data fusion hold promise. One of the major ways that we assess system safety is in terms of the human reliability analysis (HRA) that is used in probabilistic risk assessment (PRA). When conducting HRA, risk significant errors are identified, evaluated and quantified. Errors can be either slips, lapses (omissions) or mistakes. [12]. Risk estimates are input to systematic logic structures such as event trees and fault trees to support risk assessment. Combinations of hardware and human failure probabilities are propagated and uncertainty calculated with a result profile of risk produced. When calculating the human error probability, many methods assume a base failure rate that is adjusted either higher or lower based upon the status of

performance shaping factors (PSFs). Thus, the benefits to using an HRA approach over other modeling approaches lies in the identification of universal performance shaping factors, in providing logic structures that can be used in characterizing human performance within the context of plant mission and system performance (availability) and in producing error probabilities and uncertainty estimates. . However, the data underlying current human error probability estimates are not based on human performance in advanced I & C environments nor do they contain, except in a gross sense, the effects of better or worse applications of data fusion on human reliability. They also do not reflect the effects of trying to create an integrated environment fusing information representing process, cyber and physical security elements. Once human performance data for human interaction in data fusion environments is collected, human failure rates can be determined. Once this has been attained, HRA systems modeling tools will prove to be useful in characterizing and quantifying human performance in these environments.

Cognitive modeling approaches provide designers an understanding of the user's model of his/her environment. Understanding this mental model aids in the prediction of expected, plausible mission-oriented user performance. Additionally, it alerts us to the information the user will be seeking to confirm decisions and to take actions. Knowing about the mental model and information requirements can support the development of fusion basics. Designers can construct displays based upon perceptual, human information processing and psychological characteristics of users. Inference can be made regarding the user's cognitive map of the world, the type of information they anticipate and how to leverage both. Designs can then be tested and refined. For a review of the history of mental models see Johnson-Laird [13-15] For most purposes, Wickens [16] provides a usable model of cognition. Generally speaking, cognitive models can provide a basis for the design of studies to evaluate perceptual-motor interaction including the relationship of fusion to workload, awareness, semantic memory and response. These studies can help elucidate differences between preference and performance and establish data sets that can support HRA modeling. However, most cognitive models do not provide guidance for providing tailored information for fusion within a particular environment. Many do not have a wealth of underlying data. This brings us to the third complementary approach that should be employed in developing human factors guidelines for data fusion, human-in-the-loop (HITL) studies.

Often used in conjunction with human performance models, HITL studies can provide repeatable environments for testing operational scenarios. This approach to human-system performance assessment has been applied to aviation, sensor integration, and transportation domains. For example, Manning cites benefits associated with human in the loop test of automation and controls for an air traffic control environment. [17] Human in the loop studies can be used to examine human performance in the presence of fusion-aided decision aids for mixed initiative and scalable autonomy environments, two areas where we need data regarding fusion benefits. Results from these tests can be used to refine cognitive theory, provide domain specific solutions, create human reliability data for extrapolation to other environments, and help craft fused displays.

HITL has been used as in systems integration, as part of systems evaluation, and in characterizing human-environment interaction [18]. HITL testing can yield human factors principles for fusion-based design. However, HITL studies have certain weaknesses. They are relatively expensive and tend not to be used to further theory and to develop guidelines. Also, in order to transfer results to the field, the study should have the proper fidelity, that is the experimenter need know the role of the human in an operational setting, specifically what the human needs to do, sometimes when the final systems configuration is still under development. Lastly, as compared to studies of pure perception, these studies are inherently more useful because they elicit user knowledge and operating strategies, match human performance to the pace of events, incorporate the information and state uncertainty present in similar scenarios, and may include role of other personnel found in the field environment.

Employing a multi-methods approach to data fusion can offset the weaknesses of any one approach. Once the three human factors approaches above have been implemented they should help to develop repositories of information needed by designers tasked with developing fused information displays.

IV. HUMAN FACTORS ISSUES

In sufficient quantities, raw data presented to the user have the potential to overwhelm. If these data are not fused, then the user may begin to "cycle" though the data and perform the fusion process themselves [19]. There may be large differences among actors in terms of how they fuse data. This situation may be compounded by the fact that operators will process information and perform differently when data are inconsistent and conflicting. This may be the case when process conditions are changing and malicious actors are probing cyber and physical security systems. Although humans are widely adaptable, contextual elements such as the environment, pace of events, quality of procedures, efficacy of work processes, and reliability of data can serve to place the operator in a context where error can result. Under these conditions, a well crafted fusion process can help support operator decision making.

In one sense, the goals of data fusion in support of systems resilience can be construed as enhanced threat detection, positive attribution, and assessment (including

reduction in false alarms) while maintaining state awareness. These assumptions need to be empirically evaluated and the true gain from fusion evaluated. In order to improve state of the art, well crafted research studies on a variety of issues need to be conducted. Table 1 presents some topics for human factors research in with emphasis on system resilience and data fusion. For purposes of simplicity, organizational factors are not stressed. For a review of organizational factors in resilience engineering see [1]. This table is meant to be a starting point for factors worthy of consideration. For example, the introduction of data fusion within a scalable autonomy environment may be challenging. Perhaps the visual symbols presented or the parameters selected should different for different levels of autonomy. If the operator is informed of the level of autonomy he or she may be better able to prevent an emergency. A system overview may be present in both cases, but in the less automated system the designer may wish to present icons for manual actions taken and resultant changes in system status that occur. The fused representation in the more automated system would present the manual actions or their effects. In the more autonomous system, set points may be automatically changed and operators informed when automatic actions are taken.

Operator capability versus usability
Human performance under scalable autonomy
Human performance under varying levels of data fusion
Getting proper human-system performance metrics
Defining the role of data fusion in mixed initiative systems
Assessing and maintaining state awareness under dynamic conditions
Providing context-based reasoning to augment operator decision making
Maintaining data integrity
Human input to real time data mining
User controlled data scalability
Role of personnel and staffing concerns as part of resilient design
Defining and containing operator stress during process upset conditions
Operator trust in data fusion

Table 1. Human factors research topics

Operator trust in decision aiding is an area worthy of attention. For example, the potential for fused data to be corrupt can have an immense impact on operator and acceptance. Another factor could include technology acceptance including identification and assimilation with the technology. For a framework on technology acceptance see Davis [19]. In order to address these research topics a comprehensive program is required, however, even smaller efforts to address individual items could reap large benefits.

V. SUMMARY AND CONCLUSION

In the future smart systems enabled by smart designers may be able to provide operators with displays imbued with context-based reasoning thus reducing error and in many cases, manpower requirements. This will be done by extending what we know about data fusion and human information processing capability. With learning systems, it is possible that a smart system can assist the operator based on her own experience in conjunction with safety limits for operation. This calls into question not only research regarding display design, team work and distributed decision making, but how emergency response and conduct of operations is formulated.

As Ware [21] points out, aspects of visualization gain their power through a variety of means. For example, designs that leverage aspects of the human visual sensory system or that make use of symbols can facilitate perception and cognition. Methods for the study of each approach may be different. Much work in this area is still needed. To this we add practical issues when designing for resilience such as optimizing display update rates, determining end-user acceptance, consideration of short and long term memory constraints, gaining operator trust and acceptance, and applying proper functional allocation. Finally, through human in the loop testing and by making use of available human reliability models and data we can support development of the technical basis for evaluating the ability of personnel to add to system resilience in highly automated environments.

References

[1] E. Hollnagel, D. Woods, and N. Levenson, "*Resilience Engineering*," Ashgate Press, Cornwall, UK 2006

[2] G. Morel R. Amalberti, C. Chauvin, "Articulating the Difference between Safety and Resilience," Journal of the Human Factors and Ergonomics Society, Volume 50, # 1, February, 2008.

[3] D. Woods Chapter 2 in E. Hollnagel, D. Woods, and N. Levenson, "*Resilience Engineering*," Ashgate Press, Cornwall, UK 2006

[4] G. Salvendy "*Handbook of Human Factors and Ergonomics*," John Wiley InterScience, New York 1997.

[5] S. Mejdal, M. McCauley, and D. B. Beringer "Human Factors Design Guidelines for MultiFunction Displays," US Department of Transportation Federal Aviation Administration, DOT/FAA/AM-01/17 October 2001.

[6] J. Reason "*Human Error*" Cambridge University Press, 1990.

[7] US Nuclear Regulatory Commission, "Human Interface Design Guidelines," NUREG 0700, Rev 2, Washington DC 2002.

[8] MIL STD 1472 F DOD Design Criteria Standard for Human Engineering, December 2003.

[9] E. Waltz and J. Llinas "*Mutlisensor Data Fusion*," Artec House Publishers, Boston, MA 2000

[10] D. Bruemmer, D. I Gertman, and C. Nielsen, "Exploring new ways to guide human robot interaction," Cybernetics and

Systemics Journal; Vol: 1; Issue: 1, August 2007.
[11] C Nielsen, M. Goodrich and R. Ricks Ecological Intefraces for Improving Robot Teleoperation Mobility, IEEE TRANSACTIONS on ROBOTICS, VOL. 23, NO. 5, OCTOBER 2007
[12] D. Gertman , H Blackman, J. Marble, J. Byers, and C. Smith "The SPAR-H Human Reliability Analysis Method," NUREG/CR-6883, INL/EXT-05-00509, Washington DC August 2005.
[13] P. N. Johnson-Laird "Mental models and deduction," Trends in Cognitive Science, 5, pp. 434-442. 2001
[14] P. N. Johnson-Laird "Peirce, logic diagrams, and the elementary operations of reasoning," Thinking and Reasoning, 8, 69-95. 2002
[15] P. N. Johnson-Laird, Mental models, sentential reasoning, and illusionary refereces. In C. Held, and G. Vosgerau Mental Models and the Mind, New York, pp 27-52. 2006
[16] C. D. Wickens and J . McCarley *Applied Attention Theory,* CRC Press, 2007.
[17] C. Manning, Measuring Air Traffic Controller performance in high fidelity simulation, DOT/FAA/AM-00/2, Oklahoma, 2000.
[18] D. Foyle and B. Hooey. "Human Performance Modeling in Aviation," CRC publishers, 2007.392 pp
[19] R. M. Akita "User-based fusion approaches," Proceedings of the 5th International Conference on Information Fusion, Volume 2, pp. 1457-1462, 2002.
[20] F. D. Davis, R. P. Bagozzi, and P. Warshaw. "User acceptance of computer technology: A comparison of two theoretical models" *Management Science*, 35, 982-1003, 1989.
[21] C. Ware "*Information Visualization: Perception for Design*," Morgan Kauffman Publishers, Academic Press, 2000.