

A Design Rationale Capture Tool to Support Design Verification and Re-use

Becky L. Hooey¹, Jonny Carlos da Silva², and David C. Foyle³

*¹San Jose State University at NASA Ames Research Center,
Moffett Field, CA, USA Becky.L.Hooey@nasa.gov*

²Universidade Federal de Santa Catarina (UFSC), Florianopolis, Brazil,

³NASA Ames Research Center, Moffett Field, CA, USA

ABSTRACT

A design rationale tool (DR tool) was developed to capture design knowledge to support design verification and design knowledge re-use. The design rationale tool captures design drivers and requirements, and documents the design solution including: intent (why it is included in the overall design); features (why it is designed the way it is); information about how the design components support design drivers and requirements; and, design alternatives considered but rejected. For design verification purposes, the tool identifies how specific design requirements were met and instantiated within the final design, and which requirements have not been met. To support design re-use, the tool identifies which design decisions are affected when design drivers and requirements are modified. To validate the design tool, the design knowledge from the Taxiway Navigation and Situation Awareness (T-NASA; Foyle et al., 1996) system was captured and the DR tool was exercised to demonstrate its utility for validation and re-use.

Keywords: surface operations, design rationale, design verification, design re-use

1 INTRODUCTION

A wide range of new technologies are being developed to support NextGen flight deck and air traffic control operations. At the infancy of the design lifecycle, we are in a prime position to ensure that these technologies are designed in accordance with human-centered design principles. One aspect that is often overlooked is the critical need to record design rationale (DR) and the assumptions underlying the design choices, to enable design verification and to support system evolution by enabling safe changes of the design for future applications (Leveson, 2000).

Even in small projects, tracking the impact, motivation and context of individual

design decisions among designers, and over time, quickly becomes intractable. The underlying intent for the design decisions, important information about *why* the system was designed a certain way, or what design options were considered but rejected, are rarely adequately captured. Often this information is scattered throughout a collection of paper documents, project and personal notebook entries, and the memory of the designers (Klein, 1993). This makes the design rationale information very difficult to access and use, such that often this design knowledge “goes with the employee”.

Recent advances in collaborative document repositories have opened the door for new tools that facilitate and support the capture and subsequent retrieval of these critical decisions and their rationale. However, most document repositories merely store documents in a linear fashion and are inadequate because: 1) they make no attempt to ensure that the captured information is appropriate and sufficient for designers to understand, replicate, or modify the design; and, 2) they do not support design iterations – that is, if a design element or system requirement is modified, there is no easy way to propagate that change throughout the body of design knowledge, so as to understand the implications and consequences of that change.

1.1 Objectives

The specific objectives of this research were to:

1. Characterize design knowledge generated during a design process;
2. Identify post-design uses for captured knowledge;
3. Develop a prototype DR tool that enables knowledge capture and retrieval;
4. Use the DR tool to capture the Taxiway-Navigation and Situation Awareness (T-NASA) system design knowledge; and
5. Demonstrate how DR can be used for verification and re-use

2 CHARACTERIZING DESIGN KNOWLEDGE

Analyses of complex-system design projects that adhered to the National Aeronautics and Space Administration (NASA) System Engineering (SE) Process (NASA, 2007) were conducted to characterize the nature of design knowledge generated during the design of complex systems (see Hooey and Foyle, 2007). From these analyses, three categories of design knowledge were identified for inclusion in the DR tool: Design Drivers, Design Requirements, and Design Elements (also see Hooey and Foyle, 2007).

2.1 Design Drivers

Design Drivers refer to high-level design goals or philosophies and design assumptions. These drivers affect design choices; and designing to meet these drivers often requires careful analysis of design alternatives (NASA, 2007). Four kinds of design assumptions were identified (Hooey and Foyle, 2007): Operational, Technology, Usage, and Legacy. *Operational assumptions* include factors related to the expected operating environment, such as visibility and temperature. *Technology assumptions* include factors such as materials, mass, cost, and time. *Usage assumptions* consider the end-user of the system and how the system is intended to

be used. *Legacy assumptions* apply when an existing design is re-used, modified, or integrated and the legacy system is considered a ‘black-box’ that cannot be modified.

2.2 Design Requirements

Requirements are frequently established at the outset of the design project, however, they are often iterative and modified as the design progresses. As per the NASA SE process (2007), project requirements typically include functional needs requirements (what functions need to be performed), performance requirements (how well these functions must be performed), and interface requirements (design element interface requirements). Reliability, safety, environmental and human factors requirements may be included as relevant for the project. An effective requirements statement will typically include a ‘shall’ statement, metadata that may include a rationale for the requirement, and method of verification (i.e., test, inspection, analysis, and demonstration; NASA, 2007).

2.3 Design Elements

The process of defining the design solution typically includes defining alternative solutions, analyzing each solution (often using trade studies), selecting the best solution, further defining and refining the design solution, and generating a full design description (NASA, 2007). This is typically a recursive and iterative design loop guided by the design drivers and requirements. The scope of the full design description generally includes the system specifications, the functional behavior and characteristics of the physical interfaces, and the detailed build-to and code-to requirements for the end product and interfaces (NASA, 2007). Frequently, *qualifications* or caveats are placed on the design solution to indicate uncertainty, criticality, or validity of the design solution, which provide useful insights for evaluation, verification/validation, and later modifications. Finally, *alternatives that were considered, but rejected*, and the reasons why they were rejected are also important to document as they provide useful information for design modifications, or for designers of other systems (Hooey and Foyle, 2007).

3 IDENTIFYING USES OF DESIGN KNOWLEDGE

Further analysis of NASA’s SE process (NASA, 2007) highlighted two important uses of design knowledge: 1) Verification; and 2) Technology transfer / re-use. These will be the initial focus of the prototype DR tool development.

3.1 Design Verification

Design verification refers to documenting that the design is in compliance with the established design requirements as proven through performance of a test, analysis, inspection, or demonstration (NASA, 2007). To conduct design verification, one must determine if every design requirement is met, understand how each requirement is instantiated within the design, and understand the evidence offered as proof of compliance with requirements (e.g., empirical study, model analyses).

3.2 Technology Transfer and Re-use

Design rationale knowledge can be useful to support technology transfer. System developers are more likely to produce a veridical and effective version of the product in the presence of a detailed representation of the design specification. Also, fellow researchers and system designers can learn from viewing the trace of design decisions and data that led to the final design. If the original design rationale is not considered, a system could be modified for use under circumstances for which it was never intended, creating safety hazards. Unless the original designer is involved, often those carrying out the design modifications have no way to access important design assumptions and other usage constraints that are not contained in the code or visible from the finished product. As a result these are often ignored or misrepresented as the system is modified.

4 DESIGN RATIONALE TOOL PROTOTYPE

A DR tool was developed to support the tasks of: 1) *capturing design knowledge*; and, 2) *retrieving the knowledge* to support design verification and design re-use. The DR tool provides a semi-structured approach to capturing data using both symbols and text-based descriptions, and supports links between design decisions and rationale, including empirical evidence such as design standards, model output, and simulation results.

The DR tool incorporates a knowledge representation scheme that combines rules, semantic network and object-oriented modeling (see Silva, Saxena, Balaban, and Goebel, 2012 for a similar technical approach). The prototype includes two components: domain-independent rules/functions module, which includes the rules, methods and class definition, and a domain-specific instance base, which includes the knowledge related to a specific design domain.

As shown in Figure 1, the DR tool allows designers to capture high-level design drivers and requirements, and link these to each design element as relevant with rationale explaining how each driver or requirement is met by the element. The design specification for each design element includes a description (text, graphical, or video), intent (why the element was included), features (e.g., size, color, shape, material, function), qualifiers (caveats on design decisions) and alternatives considered, but rejected.

The main concepts modeled are Requirements, Elements and Rationales. An

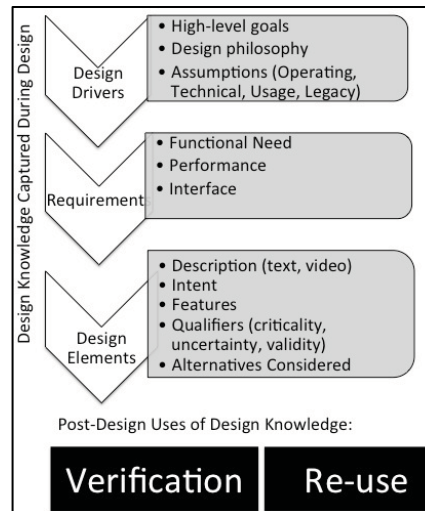


Figure 1. DR Tool knowledge captured and post-design uses.

adaptation of the Quality Function Deployment (QFD; Harty, 2001) was applied to create a class structure with a semantic network model to map the Requirements and Elements. Table 1 presents a conceptual representation of this QFD matrix. Each requirement can be satisfied by one or more elements, and each element can be related to one or more requirements, where the connections between these concepts are defined by the filled cells. Each cell corresponds to a rationale that explains why a requirement is satisfied by a particular element. The rationale may be based on empirical data or argumentation that supports the mapping between requirement-element (see section 5 for examples).

Table 1. Quality Function Deployment Matrix - Conceptual Representation

| | Element ₁ | Element ₂ | Element ₃ | ... | Element _{n-1} | Element _n |
|--------------------------|------------------------|------------------------|------------------------|-----|------------------------|------------------------|
| Requirement ₁ | | Rationale _a | | | | |
| Requirement ₂ | Rationale _b | | | | Rationale _c | |
| ... | | | | ... | | |
| Requirement _m | | Rationale _d | Rationale _e | | | Rationale _g |

A parser was developed to allow automatic knowledge acquisition by extracting information from a set of knowledge capture templates populated by the designer with design knowledge. The parser loads the templates as ASCII files, and creates instances with a semantic network linking them, consistent with the QFD method.

The semi-formal data capture process combines the freedom to document rich contexts with free-text (strings) while enabling powerful and efficient searches via symbolic manipulation. The user can interrogate the system and generate custom reports based on Drivers, Requirements, Elements, or Qualifiers. The system generates output as a set of hyperlink files, having the actual QFD matrix as an entrance point. Currently, the DR tool supports design verification and knowledge re-use (see section 5.2).

5 T-NASA APPLICATION

Using the prototype DR tool, the entire body of design knowledge of the Taxiway Navigation and Situation Awareness (T-NASA) system was captured. T-NASA is a suite of cockpit navigation displays for low-visibility airport taxi operations comprised of a head-up display (HUD) and a head-down map display (see Figure 2). T-NASA was designed using a comprehensive human-centered

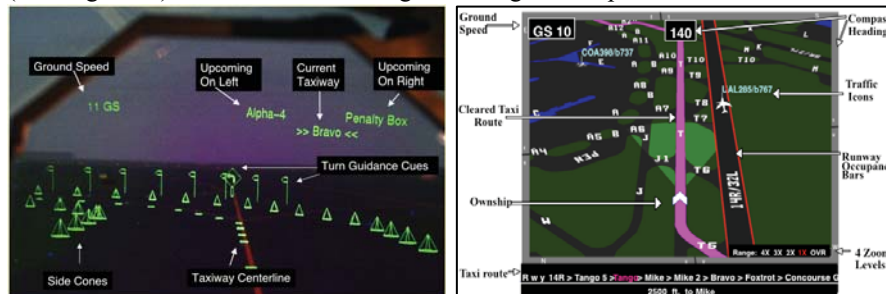


Figure 2. T-NASA HUD (left) and map (right).

design and evaluation approach that involved over 300 commercial pilots participating in part-task simulations, high-fidelity simulations, and a flight test (Foyle et al., 1996; Hooey, Foyle, and Andre, 2000). Here, the T-NASA design knowledge was captured retrospectively; however, it is expected that the DR tool would be used throughout the design process and as such would be integrated with design, collaboration, and communication tools to reduce the burden of documentation.

5.1 T-NASA Knowledge Capture

The following provides examples of T-NASA design knowledge that was captured using the prototype DR tool.

5.1.1 T-NASA Design Drivers. In the T-NASA design example, two types of design drivers guided the design process. High-level design philosophies are presented in Table 2 and the four categories of design assumptions are presented in Table 3.

Table 2. Examples of T-NASA Design Goals (Foyle, Andre, and Hooey, 2005)

| <i>Philosophy</i> | <i>Description</i> |
|------------------------------|---|
| Maximize Eyes-Out Time | The map should be used to support global awareness only, and not local guidance, as the latter would require the pilot to taxi the aircraft in an "eyes-in, head-down" mode. |
| Minimize Attentional Capture | Where possible, the HUD should present conformal symbology that is superimposed on the world, overlays real-world objects, and preserves angular measurements. Studies (Wickens and Long, 1995) have shown that non-conformal graphical HUDs may lead to attentional tunneling, causing pilots to miss unexpected environmental events and may induce higher workload due to cognitive switching between the world and symbology. |
| Visual Momentum | Because the T-NASA system is comprised of two coordinated displays, there is a need to keep the pilot oriented when scanning among the real world, HUD, and map. The design concept of <i>visual momentum</i> (Woods, 1984) was used to enable these transitions: Corresponding display components appear in both the HUD and map, and correspond to the real world components. |

Table 3. Examples of T-NASA Design Assumptions (from Foyle et al., 1996)

| <i>Assumption</i> | <i>T-NASA examples</i> |
|-------------------|--|
| Operating | Low visibility (~ 650 ft runway visual range; not zero visibility) |
| Usage | Two-pilot crews; commercial transport aircraft |
| Technology | Aircraft equipped with: left-side HUD, datalink, electronic surface map, Differential Global Positioning System (GPS), and ASDE-3 RADAR. |
| Legacy | Standard cockpit display configuration |

5.1.2 T-NASA Design Requirements. The T-NASA designers (Hooey, Foyle, and Andre, 2000) identified three types of information requirements: 1) Local Control; 2) Route Guidance; and, 3) Global Awareness, which were further divided

into more specific sub-requirements (see Table 4).

Table 4. Examples of T-NASA Design Requirements

| <i>Requirement</i> | <i>Sub-Requirements</i> | <i>Description</i> |
|--------------------|-------------------------|---|
| Local Control | Lateral Control | Guidance to minimize lateral deviations |
| | Directional Control | Guidance to negotiate turns |
| | Longitudinal Control | Guidance for speed and braking |
| | Hazard Detection | Support monitoring for traffic/obstacles |
| Route Guidance | Ownship Position | Knowledge of position |
| | Hold Location | Location of, and distance to, hold bar |
| | Cleared Route | Name of required taxiway, distance to turn, direction of turn |
| Global Awareness | Airport Layout | General layout of airport |
| | Landmarks | Location of gate or runway |
| | Traffic Awareness | Awareness of flow of traffic |

5.1.3 T-NASA Design Elements. Thirteen design elements were identified. For each element, detailed design knowledge was captured to populate the attributes presented in Figure 1. Where applicable the rationales are linked to supporting evidence such as industry standards or guidelines (e.g., FAA advisory circulars), empirical studies, or previous literature. Figure 3 shows the design specifications captured for one T-NASA design element, the ‘*traffic icon*’.


| Traffic Icon | | |
|--|--|---|
| Description | Design Features | Features Rationale |
| Aircraft symbols depicting traffic location on airport | Located on Map (not HUD) | The map's 360 deg. view of airport allows all traffic to be depicted. The HUD's minimal field of view prohibits a veridical display of traffic |
| Intent Rationale | Color | White (FAA, 2011; AC 20-172) |
| Provide pilots with increased awareness of traffic in low-visibility conditions and support traffic sequencing (knowing which aircraft to follow or cross behind). | Not to scale | Discourages pilots from using map to judge clearance from another aircraft. |
|  | Data tag | Aircraft identifiers help traffic sequencing (Andre, 1995) |
| | Declutter Mode | Increases legibility in high traffic |
| | Two-stage alert | Yellow warnings indicate potential traffic threats. Red alerts require immediate action. Consistent with current standards (FAA, 2011; AC 20-172) |
| | Design Drivers | Design Drivers Rationale |
| | Minimize eyes-in-time | Does not depict accurate wingspan to discourage pilots from relying on map to determine clearance for passing |
| Design Qualifier | Design Qualifier Rationale | |
| Criticality | Level = high Minimize incursions and increase runway safety | |
| Alternatives | Reason for Rejecting | |
| Oval Shape | Used when map update rate is slow and/or direction of travel is unknown (FAA, 2011; AC 20-172) | |

Figure 3. Design Element Rationale used for Technology Transfer.

5.2 Knowledge Retrieval

With the DR tool fully populated with the T-NASA design knowledge, the utility of the design knowledge for design verification and re-use was explored.

5.2.1 Design Verification

The QFD matrix generated by the DR tool is shown in Table 5. Each design element (columns), requirement (rows) and rationale (individual cells) is a hyperlink that accesses deeper design knowledge. The matrix shows that each T-NASA requirement was satisfied by one or more elements, and each element was related to one or more requirements. Each filled cell corresponds to a requirements rationale, and the user can select it to drill-down to understand how a requirement is satisfied by a particular element.

Table 5. T-NASA Qualify Function Deployment Matrix

| Requirements | HEAD-UP DISPLAY (HUD) | | | | | MAP | | | | | | | |
|-------------------------|----------------------------------|---------------------------------|---------------------------------|----------------------------------|----------------------------------|----------------------------------|---------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|-----------------|----------------------------------|
| | Route Markings | Taxiway Label | Ground Speed | Hold Bar | Turn Flags | Airport Map | Ownship Icon | Magenta Route | Taxi Clearance | Hold Bar | Traffic Icon | Compass Heading | Runway Occupancy Bars |
| Local Control | | | | | | | | | | | | | |
| Lateral control | Rat₁ | | | | | | | | | | | | |
| Directional control | | | | | Rat₂ | | | | | | | | |
| Longitudinal control | Rat₃ | | Rat₄ | | | | | | | | | | |
| Hazard detection | | | | | | | | | | | Rat₅ | | Rat₆ |
| Route Awareness | | | | | | | | | | | | | |
| Ownship position | | Rat₇ | | | | | Rat₈ | | Rat₉ | | | | |
| Cleared route | Rat₁₀ | | | | | | | Rat₁₁ | Rat₁₂ | | | | |
| Distance to turn | | | | | | | | | Rat₁₃ | | | | |
| Direction of turn | Rat₁₄ | | | | Rat₁₅ | | | Rat₁₆ | | | | | |
| Hold location | | | | Rat₁₇ | | | | | Rat₁₈ | Rat₁₉ | | | |
| Global Awareness | | | | | | | | | | | | | |
| Airport layout | | | | | | Rat₂₀ | | | | | Rat₂₁ | | |
| Runway location | | | | | | Rat₂₂ | | | | | | | Rat₂₃ |
| Traffic awareness | | | | | | | | | | | Rat₂₄ | | Rat₂₅ |

Note: Rat = Rationale

Further, by selecting a requirement (left column, Table 5), the DR tool will return a list of all design elements that support the specified requirement and the associated rationale that describes how the design element supports the requirement. Figure 4 shows the output produced if one chooses to investigate the requirement *Hazard Detection*. As can be seen, the requirement of supporting *Hazard Detection* is met by the elements *traffic icon* and *runway occupancy bars* on the map.

| Design Elements | Requirements Rationale | |
|-----------------------|---|--|
| Traffic Icon | Two-stage alerts. Traffic icon turned yellow to warn of a potential threat, red to alert of impending danger | |
| Runway Occupancy Bars | It is important to show when the runway is occupied due to severe safety consequence of taxiing onto an active runway. Red highlight was a strong visual cue to remind pilots not to taxi onto runway. This feature was also found to be useful for pilots of landing aircraft who checked if runway was clear for landing. | |

Figure 4. Design Requirement Rationale used for Design Verification

5.2.2 Design Re-Use

The DR tool can support design re-use by identifying which design elements are affected if critical design drivers are modified. As the design progresses, design elements can be linked to the design drivers to allow users to trace how design drivers are instantiated among the design elements. For example, the need to *Maximize Eyes-out Time* was deemed important by the T-NASA designers for the intended user-group of commercial aircraft pilots taxiing at busy, congested, airports. However, if the T-NASA design was applied to another application that does not share this requirement, (e.g., a future jetliner that replaces forward-facing cockpit windows with computer-generated synthetic vision displays), then it would be important for the designers of this future system to understand which aspects of the T-NASA design might be affected.

| Maximize Eyes-out Time | T-NASA Elements | Design Instantiation to Maximize Eyes-Out Time | Alternatives considered but rejected |
|------------------------|-----------------------|--|---|
| | Traffic Icon | Pilot-selectable declutter feature only shows traffic icons that pose a threat to ownship | Accurate wingspan NOT depicted to discourage pilots from using map to determine clearance |
| | Runway Occupancy Bars | Pilots can determine runway occupancy status with a quick glance at the map | Yellow bars at taxiway intersections – could be confused with holdbars |
| | Ownship Icon | Icon is in fixed location, while map background moves and rotates, eliminating the need to search for icon on map. | Speed and turn predictors NOT included to prevent use for closed-loop control |
| | Magenta Route | Thick ribbon discourages pilot from using map to track centerline | Taxiway centerline NOT shown |

Figure 5. Design Driver Rationale used for Design Re-Use.

Similarly it is important to identify design elements that were considered but rejected. These are provided in the right-most column of Figure 5. For example, the T-NASA designers purposefully did not provide precision control information, such as speed and turn predictors, to prevent the pilot from taxiing in a head-down position and from attempting to make closed-loop control decisions with a low-resolution, non-conformal display as this would directly violate the intended usage and design philosophy. However, this information may very well be needed with a full synthetic vision display used under different operating conditions.

6 Conclusion

A knowledge-based system to capture design rationale was developed and tested by capturing design knowledge gathered from the T-NASA display suite. The DR tool was capable of documenting the main design concepts of the T-NASA design. The tool supported comprehensive data capture guided by input templates that adhered to the SE process. It also supported efficient retrieval of the knowledge for design verification, technology transfer, and re-use in ways not previously possible

with most current document repositories.

The value of a DR tool depends on the quality of the design knowledge that is captured by members of the design team. Such a tool will only be adopted by designers if it provides some intrinsic value to the individual designer such as facilitating trade studies and fulfilling formal design review requirements. Embedding multiple, easy-to-use input methods such as ‘drag-and-drop’ and ‘save-to-archive’ options within existing design tools (e.g., CAD tools, prototyping tools) and communication methods (e.g., e-mail, instant messaging, smart pens, electronic whiteboards) will be important for supporting data capture without excessively burdening the designer.

ACKNOWLEDGMENTS

The design rationale tool was developed under joint funding by the NASA Aviation Safety Program, System-wide Safety Assurance: Human Systems Solutions and CAPES Foundation, Brazil (Grant 4095/10-3).

REFERENCES

- Federal Aviation Administration (FAA). 2011. Airworthiness Approval for ADS-B in Systems and Applications (Advisory Circular 20-172). Washington D.C.
- Foyle, D. C., A. D. Andre, R. S. McCann, E. M. Wenzel, D. R. Begault, and V. Battiste 1996. Taxiway Navigation and Situation Awareness (T-NASA) System: Problem, design philosophy and description of an integrated display suite for low-visibility airport surface operations. *SAE Transactions: Journal of Aerospace*, 105, 1411-1418.
- Foyle, D. C., A. D. Andre, and B. L. Hooley. 2005. Situation Awareness in an Augmented Reality Cockpit: Design, Viewpoints and Cognitive Glue. *Proceedings of the 11th International Conference on Human Computer Interaction*. Las Vegas, NV.
- Harty, D. 2001. Quality Function Deployment- An Overview of QFD and its Applications to Software Engineering. Accessed December 1, 2011, <http://www.dharty.com/erau/530-requirements/QFDPresentation/DhartyQFD.pdf>
- Hooley, B. L. and D. C. Foyle. 2007. Requirements for a Design Rationale Capture Tool to Support NASA’s Complex Systems. *International Workshop on Managing Knowledge for Space Missions*. Pasadena, CA.
- Hooley, B. L., D. C. Foyle, and A. D. Andre. 2000. Integration of cockpit displays for surface operations: The final stage of a human-centered design approach. *SAE Transactions: Journal of Aerospace*, 109, 1053-1065.
- Klein, M. 1993. Capturing design rationale in concurrent engineering teams. *IEEE Computer Journal. Special Issue on Computer Support for Concurrent Engineering*, 26(1), 39-47.
- Leveson, N. 2000. Intent Specifications: An approach to Human-Centered Specifications. *IEEE Transactions on Software Engineering*, 26(1), 15-35.
- National Aeronautics and Space Administration (NASA). 2007. NASA Systems Engineering Handbook (NASA /SP-2007-6105, Rev 1). Washington, D.C.
- Silva, J. C., A. Saxena, E. Balaban, and K. Goebel. 2012. A Knowledge-Based System Approach for Sensor Fault Modeling, Detection and Mitigation. *Expert Systems with Applications*. Accessed April 17, 2012, <http://dx.doi.org/10.1016/j.eswa.2012.03.026>
- Wickens, C. D. and J. Long. 1995. Object vs. space-based models of visual attention: Implications for the design of head-up displays. *Journal of Experimental Psychology: Applied*, 1, 179-194.
- Woods, D. D. 1984. Visual momentum: A concept to improve the cognitive coupling of person and computer. *International Journal of Man-Machine Studies*, 21, 229-244.