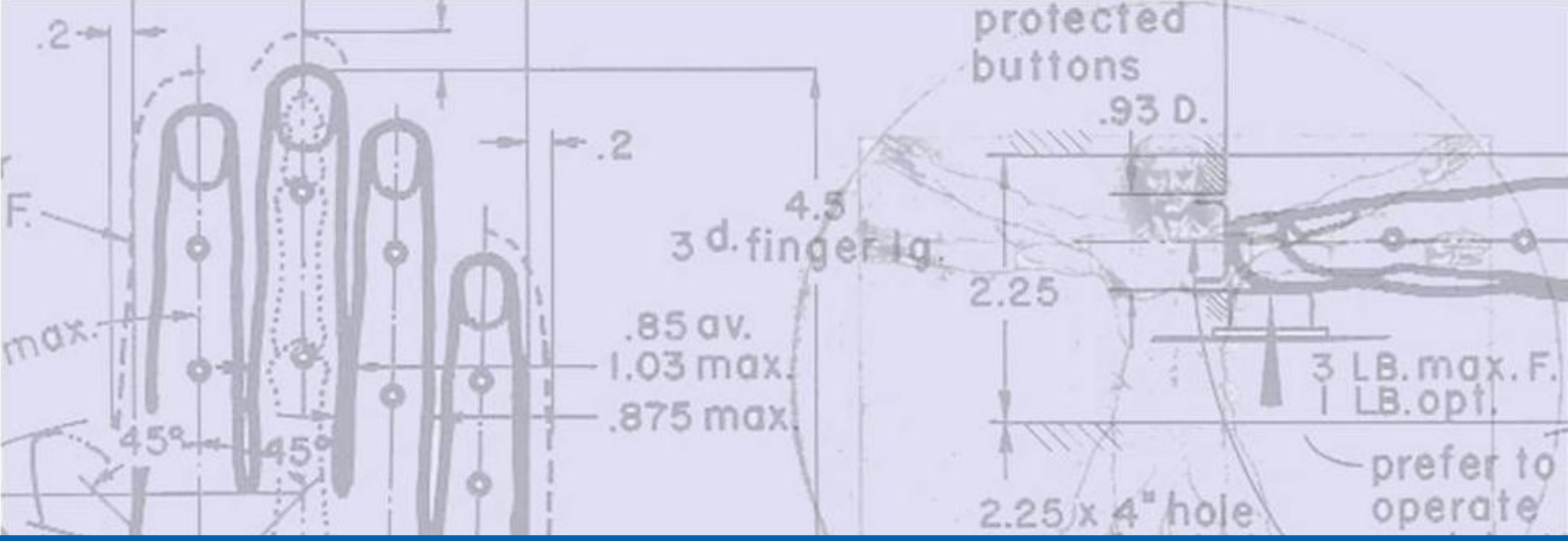


HUMAN RESILIENCE: SCOPE AND CONSIDERATIONS

HSI Panel on the Human Contribution to Resilient Systems

Matthew Risser, Ph.D.

Pacific Science & Engineering Group, Inc.

NDIA 14th Annual System Engineering Conference, October 24-27, 2011

Background

- Operations are increasingly distributed and decentralized
- Increasing reliance on net-centric, system of systems (SoS)
- Human operators are an integral part of these complex systems
  - Decode disparate data into consolidated information to support decision-making
- Current system development processes are structured to deliver a future solution based on today's requirements
- Traditional system design approaches have focused on failure prevention in contrast to designing for uncertainty

Resilience

- In many old, rigid (non-resilient) systems, the unstated expectation is that the human will provide ALL of the resilience needed by the overall (man-machine) system in order to accommodate the full range of operational conditions, uncertainties, and failures
- This human resilience requirement is typically met via training and simulations (e.g., unplanned emergencies or conditions in a training exercise)
- The challenge now is to understand the range of operating conditions (e.g., system interdependencies, degrees of automation) that give rise to the need for system resilience, and the extent of tolerance required
- Its a “function allocation” problem. Namely, who (man or machine) should be responsible for assuring system resilience – and under what conditions and to what extent?

Resilience Engineering – An HSI Perspective

- Resilience engineering proposes that we must better understand ‘how and why’ things go right – to better enable a system to function under any condition and improve the probability for success
- Resilient systems have the ability to adjust functions prior to, during, or following expected and unexpected changes to sustain operations
- Specifically, resilient systems must possess the ability to know what to do, know what to monitor, know what to expect, and know what has happened (Hollnagel, et. al., 2010)
- This implies that the function allocation between humans and machines requires some degree of malleability which has significant implications for the role of the human, and their contribution to total system performance

Outline

- Human Performance
- System Defenses
- Function Allocation
- System of Systems
- Design Implications
- Way-Forward

Human Performance - A Resilient View

- **Concept**
  - Resilience engineering enables a proactive approach to identify the relevant human performance factors that need to be accommodated during system design
- **Considerations**
  - **Workload** – resilient systems may increase user workload when users are required to assume a new function where timing and disruptions are also a factor
  - **Error Recovery** – in a resilient system, system state changes and reallocation of functions may result in delayed or undetected human error
  - **Cascading Consequences of Error** – undetected errors, uncorrected errors, or even multiple small errors can have negative downstream effects on total system performance, which is more likely to occur within a SoS environment
  - **Expertise and Training** – resilient system designs will require users to have the knowledge, skills, and abilities to adapt and perform a wider range of tasks
  - **Situation Awareness** – in dynamic and complex environments, the system must communicate and enable the user to anticipate change
  - **Decision-making** – the system must provide relevant contextual information regarding system state changes
  - **Automation and Trust** – when poorly implemented, adaptive automation can negatively impact the user's preparedness to assume a new function and reduce trust in the system

Human Performance (cont.)

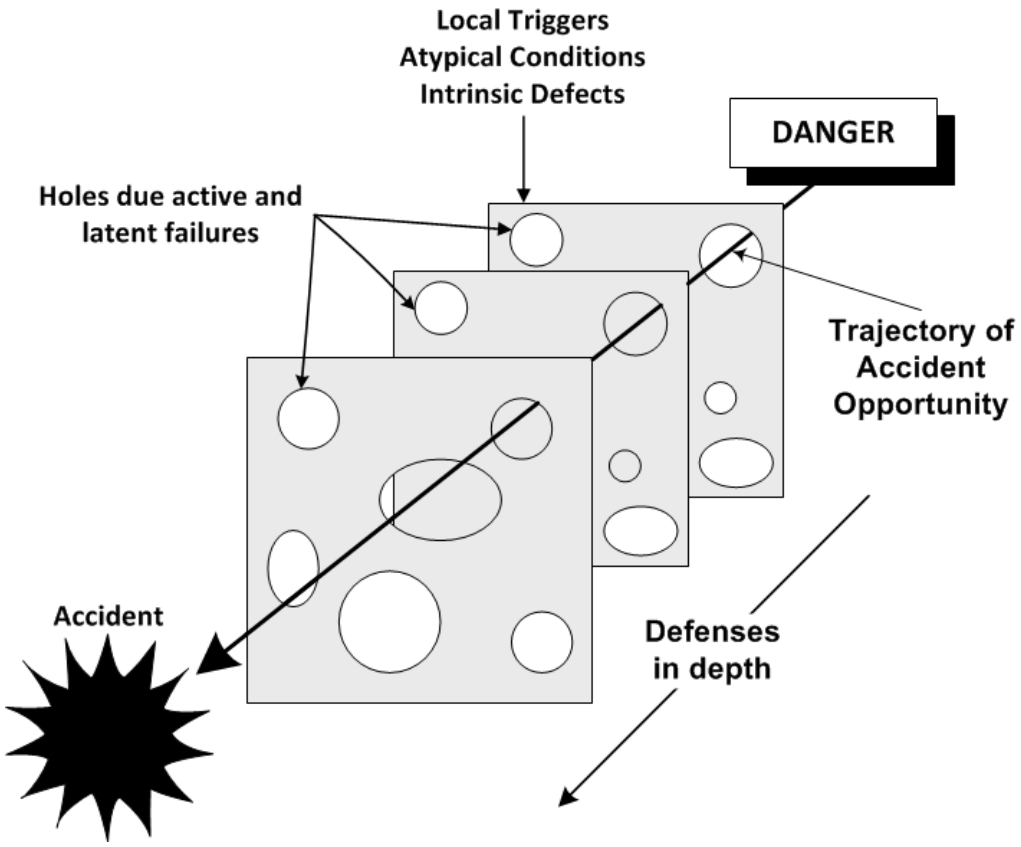
- **Recommendations**
  - Model and mitigate the consequences of compounding, delayed, or undetected errors
  - Communicate awareness of failure states, impending function changes, and alternative courses of action
  - Need to consider system failure states and function reallocation tasks for resilient training analyses /solutions and personnel determinations
  - Determine user needs for relevant contextual information
  - Use adaptive automation to reallocate functions to the human, yet provide meaningful information to the user to facilitate trust in the automation

System Defenses – More than Human

- **Concept**
  - Major disasters are rarely, if ever caused by one factor, either technological or human
  - Organizational errors are the result of failed defenses caused by complex interactions among humans, technology, and organizational influences
- **Considerations**
  - System defenses are measures aimed at removing, mitigating, or protecting against operational hazards
  - Latent Failures - unnoticed and lay dormant within a system; tolerated, detected, and corrected by protective measures (defenses)
  - Active Failures - provides a trigger for the latent failures to penetrate the defenses
  - An emergent property of any complex system includes risk balanced between latent errors in the system and its defenses – resilient system design must manage these uncertainties and risks

Failures in System Defenses

- An accident trajectory that penetrates system defenses at only a rare opportunity where failure has occurred at each structure (or subsystem) at a specific time and place
- This represents the complex interaction of latent failures and local triggering events
- An ideal system state would include the local triggers and defenses without the “holes” caused by latent and active failures
- Resilient systems must assess these organizational defenses, and plan for failures as part of the design



Adapted from adapted from Reason (1990; 1997)

System Defenses (cont.)

- **Recommendations**
  - From a sociotechnical perspective, there is a need for a paradigm shift in dealing with the safety and operation of complex technological systems
  - Reducing the likelihood of failure in complex systems requires a holistic, integrated, and multidisciplinary design approach where equal attention should be given to each element or subsystem
  - Analyze and understand the interdependencies among a system and its sub-system's defenses to interpret the likelihood of error

System of Systems - Dynamic Consumers

- **Concept**
  - Resilient systems and their users will have dependencies on other systems and the emergent properties of those interdependencies will influence total system performance, amplifying the need for resilience engineering
- **Considerations**
  - Design modifications or errors in one system may exert unintended consequences on other system(s)
  - There may be secondary and unintended users that are dependent on the outputs of that system
  - Complexity increases for function allocation assignments, taking into account the combinations of personnel, equipment, operational influences, and system interdependencies
  - Need to minimize disruptions (or capitalize on opportunities) to the user as one system in a SoS is degraded
  - Identify user-centered SoS issues, including interface design elements, navigation across systems, and awareness of one's location within the SoS

System of Systems (cont.)

- **Recommendations**
  - Ensure requirements and design analyses account for downstream or unintended users
  - Model the user workflow, user information needs, and potential failure states across interdependent systems
  - Identify synchronization requirements across the systems in a SoS, e.g., timely information exchanges, operator workload distribution, delays in updating situation awareness

Function Allocation – Changing the Human Role

- **Concept**
  - Currently, function allocation is determined early in the lifecycle and remains relatively fixed throughout system development
  - The adaptive nature of resilient systems reallocates system functions to the human which changes their role
- **Considerations**
  - From a human factors perspective, there are two automation frameworks to support function allocation
    - Sheridan and Verplank (1978) propose 10 levels of automation and allows for fine distinctions between human and machine roles
    - Folds and Mitta (1995) propose 4 levels of automation which allows for more degrees of freedom between human and machine roles
  - Human operators need to understand the priority of the reallocation and the anticipated duration to manage workload
  - Transfer of functions from the system to human needs to be seamless and stable while keeping the human in the loop

Function Allocation - Levels of Automation

Sheridan & Verplank, 1978

1. Automated system offers *no assistance*, the human performs all operations
2. Automated system offers a *complete set of action alternatives*
3. Automated system *narrows the selection* down to a few
4. Automated system *suggests a selection*
5. Automated system *executes suggestions after operator approves*
6. Operator can *overrule automation decision* automatic execution
7. Automated system *performs automatically then necessarily informs* the operator
8. Automated system *informs the operator after execution* only if he asks
9. Automated system informs the operator after execution implementation and *only informs operator of performance if system deems it necessary*
10. Automated *system decides everything and acts autonomously*, leaving the operator completely out of the loop

Folds & Mitta, 1995

1. *Direct Performer* - human performs all info processing
2. *Manual Controller* - decision making reserved for human
3. *Supervisory Controller* - machine (often software) can make decisions, but human can override machine
4. *Executive Controller* - machine performs all processing, human only starts/stops execution

Function Allocation (cont.)

- **Recommendations**
  - Determine thresholds for adaptive automation to reallocate functions
  - Enable function allocation procedures some degree of flexibility to support temporary function reallocation
  - Determine requirements to ensure a usable approach to function reallocation
  - Communicate function priority and estimated duration to the user

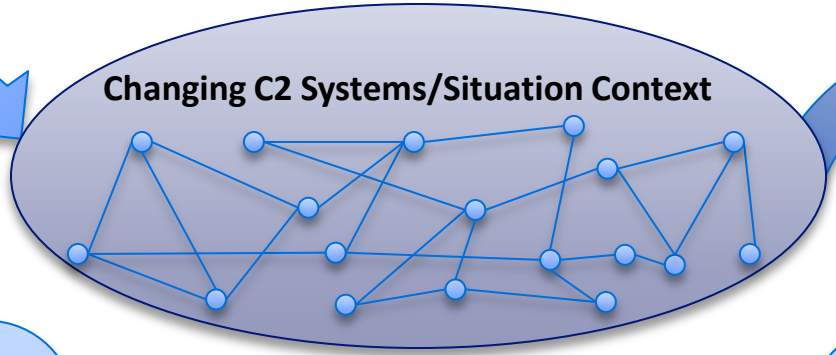
Implications - Designing for Resilience

- **Concept**
  - To ensure a system is resilient, it must effectively communicate varying states of uncertainty, emergent operational conditions, and function reallocation to the human operator to ensure it remains consistent with intended system goals
- **Considerations**
  - **Contextual information** – to improve human performance during state changes, resilient systems should provide information about the reason for change, anticipated duration, and mission or environmental conditions
  - **Supervisory displays** – enables the user to monitor systems, sub-systems, or system elements to anticipate changes and manage workload
  - **Alerting** – cues the operator to impending or immediate state changes or failures to better manage their workload and reduce errors
  - **Adaptive interfaces and visualization** – dynamically provides relevant user interfaces and visualizations that are situation dependent to improve response times and decision-making
  - **Comparative analysis** – during state changes or failures, resilient systems should propose alternate Courses of Action (COAs) based on mission impacts to improve operator decision-making

Implications (cont.)

- **Recommendations**
  - Identify and address human performance risks by using appropriate user-centered design solutions
  - Provide the relevant status and contextual information to ensure operators have total system SA
  - Facilitate the understanding of consequences resulting from system state changes
  - Communicate the purpose, priority, and duration of a function reallocation
  - Provide the operator with adaptive interfaces and course correction alternatives to improve the probability of success

Example of a User-Centered Resilient Design



Adaptive Command Visualization

- Adaptive representation of alternative COA's for dynamic assessment of mission impacts to determine optimal COA
  - Including reprioritization of tasks to achieve mission success
  - Timelines (Impact of system degradation compared against the alternative COA)
- Optimal information representation for each type of display platform
- Representation of collaborative nodes
- C2 Vulnerabilities

User Profile (Goals and Intents):

- User Role
- Decision biases
- Prioritizing and Risk Assessment
- Anticipation of Change/SA
- Collaboration requirements
- Trust in Automation

Adaptive Control Interface

- Adapting current state based on health and status of sensors/networks/environments
  - Alerting
- COA [thresholds] based on the particular type of mission
  - Prioritization of mission and associated tasks
- Deep Reflection
  - Linkages between systems
  - Computation of 1st, 2nd, and 3rd order effects (including time(s) of effect or degradation over time)
  - Geographical Space considerations (resource allocation)
- Levels of automation (to allocate functions between the user and system)

The user profile tailors the representation of information from the adaptive interface into an adaptive visualization providing decision support in a degraded C2 environment.

Adapted from King, M.A & Risser, M.R. (2011). Pacific Science & Engineering Group (for DARPA Resilient C2 Program)

Implications for System Engineering Phases

- Analysis
  - Assess complex interactions among operational conditions, system states, and identify user needs from multiple systems
- Requirements
  - Develop conditions and thresholds for adaptive function reallocation
- Design and Develop
  - Design adaptive interfaces to support the human operator
- Test
  - Evaluate both human and total system performance under varying operational conditions and system failure states

Summary and Impact

- Resilience engineering will require a multi-disciplinary approach to not only accommodate perturbations within the planned design, but also a subset of possible deviations external to the system boundaries
- Resilience engineering in complex systems must consider:
  - Human performance risks
  - Organizational defenses
  - Malleable Function Allocation
  - System complexity and interdependencies (in SoS)
  - Adaptive user-centered design strategies
- Human performance benefits of resilience engineering:
  - Uses a proactive vs. reactive design approach
  - Improves awareness of significant events before or as they happen
  - Supports the dynamic reallocation of functions between man and machine to maintain total system performance

Challenges for Discussion

- Develop or modify tools to support the engineering process
  - Do we need to develop analysis procedures to support future “what if’s” (e.g., CONOPS, capabilities, user needs)? How do you bound the extent or scope?
  - Can we modify existing analyses or must we develop methods to determine operating conditions and triggers for function reallocation?
- Improve function allocation process
  - How would we categorize and determine dynamic function assignments during the requirements phase? What should it be based on – mission scenarios, probability of failure?
  - How do we operationalize thresholds for function reallocation?
  - When and how will the human return the function back to the system?
  - How can M&S support?
- Develop user-centered adaptive interface design strategies
  - How do you communicate priority of a function reassignment?
  - How do you facilitate impending or real-time transfer of responsibility?
  - How do you communicate the contextual information associated with a system state change?
- Design test events to assess total system and human performance in dynamic environments under various uncertainty and failure conditions
  - How do we introduce and test for uncertainty?
  - How do we determine the optimal combination and number of test scenarios?

Contact

For more information please contact:

Pacific Science & Engineering Group
9180 Brown Deer Rd
San Diego, CA 92121
(858) 535-1661
www.pacific-science.com

Matthew Risser, Ph.D.