The Human Role in Resilience Engineering: A Practical View

Presented by:

Elaine M. Thorpe
Technical Fellow
The Boeing Company
elaine.m.thorpe@boeing.com

NDIA 15th Annual System Engineering Conference, October 22-25, 2012

12-00998-EOT

Talking Points

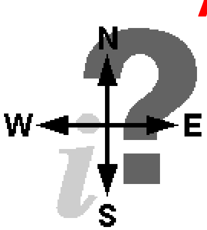
- Background
- Cornerstones of Resiliency
- A Practical View of Resilient Human Interface Design
- Continuum of Allocation & Control Levels
- Impact to HSI Design Process
- Impact to Acquisition Life Cycle
- Summary & Wrapup

Background

- Human operators are an integral part of today's complex systems, which are increasingly distributed, decentralized and interoperable (Risser, 2011)
- Traditionally, we are asked, what is the human's contribution to system error, and how do we assign a metric, $P_{err} = 10^{-X}$?
- Methodologies in Human Reliability Assessment (HRA) have been developed and traded (Chandler, et. al., 2006)
  - Most methods are based on physical action - button presses, switch actuation
  - Few methods incorporate the cognitive aspect of HRA
- Rather than focus on P_{err}, resilient systems focus on what went right (Hollnagel, 2011)
  - Specifically what role did the human operator play in making a positive contribution within an integrated system
- Allocation of functions between the human operator and automation is fluid and context specific in highly resilient systems, *but…*

How Much Does it Cost?

Does our Methodology Need to Change?



4 Cornerstones of Resilience

- Abilities Needed for System Resilience (Hollnagel et. al; 2011)
  - Knowing what to do, *How to respond to events*
    - Addresses the ‘actual’
  - Knowing what to look for, *Monitoring current events and near term ‘threats’*
    - Addresses the ‘critical’
  - Knowing what to Expect, *Anticipating potential threats and opportunities further into the future*
    - Addresses the ‘potential’
  - Knowing what has happened, *Learn from past failures and successes*
    - Addresses the ‘factual’

A Practical View of Resilient Human Interface Design

As systems and environments become more complex, resilient human-system interfaces are needed to provide the following design enablers:

- Flexible and unscripted task share between human operators and automated processes
- Facilitate a good display suite providing Situation Awareness regarding
  - Current system modes and states
  - Clarify who is in charge
  - Promote safety due to reduced human error
- Require malleable system architectures and software design
- Allow human operators and software to back each other up
  - Leader-follower roles
  - Luke Skywalker and R2D2--the perfect state
- Optimize human-automation task-share to achieve
  - Increased Safety due to reduced human error
  - Reduced manning which reduces life cycle costs
- Applications include
  - Complex cockpits/crewstations, health care, manufacturing, nuclear power plants

Continuum of Allocation & Control Levels

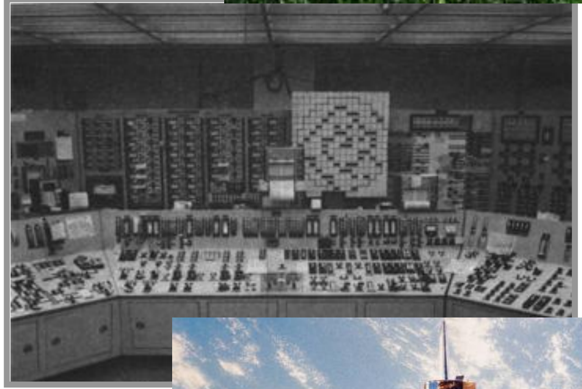
Fully Manual ↑↓ **Fully Auto**

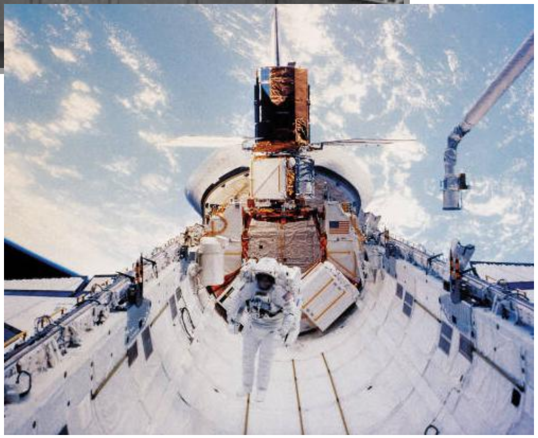
Function Allocation Levels of Automation			
Sheridan & Verplank (1978)	**Folds & Mitta (1995)**	**Case Study** What went Wrong	**Case Study** What went Right
1. Automated system offers *no assistance*, the human performs all operations	*1. Direct Performer* - human performs all info processing	3 Mile Island Incident	
2. Automated system offers a *complete set of action alternatives*	*2. Manual Controller* - decision making reserved for human		Apollo Spacecraft
3. Automated system *narrows the selection* down to a few		USAir Flt 1549, Ditch into Hudson River	Space Shuttle
4. Automated system *suggests a selection*			
5. Automated system *executes suggestions after operator approves*			Route Replanner Commercial & Military Aircraft
6. Operator can *overrule automation decision* automatic execution	*3. Supervisory Controller* - machine (often software) can make decisions, but human can override machine		
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*	*4. Executive Controller* - machine performs all processing, human only starts/stops execution	Soyuz Capsule Accident	UAVS Driverless Cars
10. Automated *system decides everything and acts autonomously*, leaving the operator completely out of the loop			Airport Trams

- Adapted from Risser, 2011

Example 1: *The 3 Mile Island Incident*

- Highly Manual System (direct performer)
- Reliance on Human Operators to Quickly:
  - Trouble Shoot what went wrong
  - Make Decisions in noisy environment with faulty data
  - Discern banks of Manual Switch settings
    - Commanded vs Actual Disagreement
  - Poor Situation Awareness





The setup: *1979, 3 Mile Island Nuclear Power Plant, near Hershey PA.*
- Temporary clog in feedwater lines of turbine 1. One second later, redundant safeguards began supplying an alternate source of feedwater.

-The sequence of certain events - - equipment malfunctions, design-related problems and human errors - - led to significant damage to the TMI-2 reactor core but only very small off-site releases of radioactivity.

The Outcome: *Led to improved Regulatory Oversight in Nuclear Power Plant Industry*

Example 2: *USAir Ditched in Hudson River*

- Auto- Manual System (manual & supervisory controller)
- Success Determined by Human Serendipity
  - Capt Sully drew from life experiences as fighter & glider pilot
  - Time-constrained 'all or nothing' decision to make
  - Disengaged auto controls
  - Perfect Airmanship by Crew
    - Wings level, nose slightly raised, pull remaining power
    - "Brace yourselves because we're going down"
- Good Weather, Over Water Safety Equipment

The setup: *2009, USAir Flt 1549, encounters birdstrike event resulting in dual engine failure on climbout from La Guardia airport enroute to SEATAC via Charlotte.*
- Full fuel, losing airspeed and altitude, crowded airspace over metropolitan area

-Capt Sullenberger assesses options: return to airport, proceed to KTEB, or land in river

The Outcome: *Makes controlled belly landing into water, in proximity to rescue boats. All passengers & crew survived.*

"This emergency ditching and evacuation, with the loss of no lives, is a heroic and unique aviation achievement.. It is the most successful ditching in aviation history". Guild of Air Pilots & Air Navigators

Example 3: *Soyuz-11 Capsule Decompression*

- Fully Automated (executive controller)
- Reliance upon software with little crew control
  - No integrated Alerting system
  - 3 Cosmonauts crowded into module sized for 2
  - Not wearing pressure suits
  - Lack of rigor in Task/Function analysis
    - Explosive bolts in proximity to crew hatch & pressure valve
    - Pressure Valve handle unusable in emergency situation
- Lack of Situation Awareness Doomed the Crew

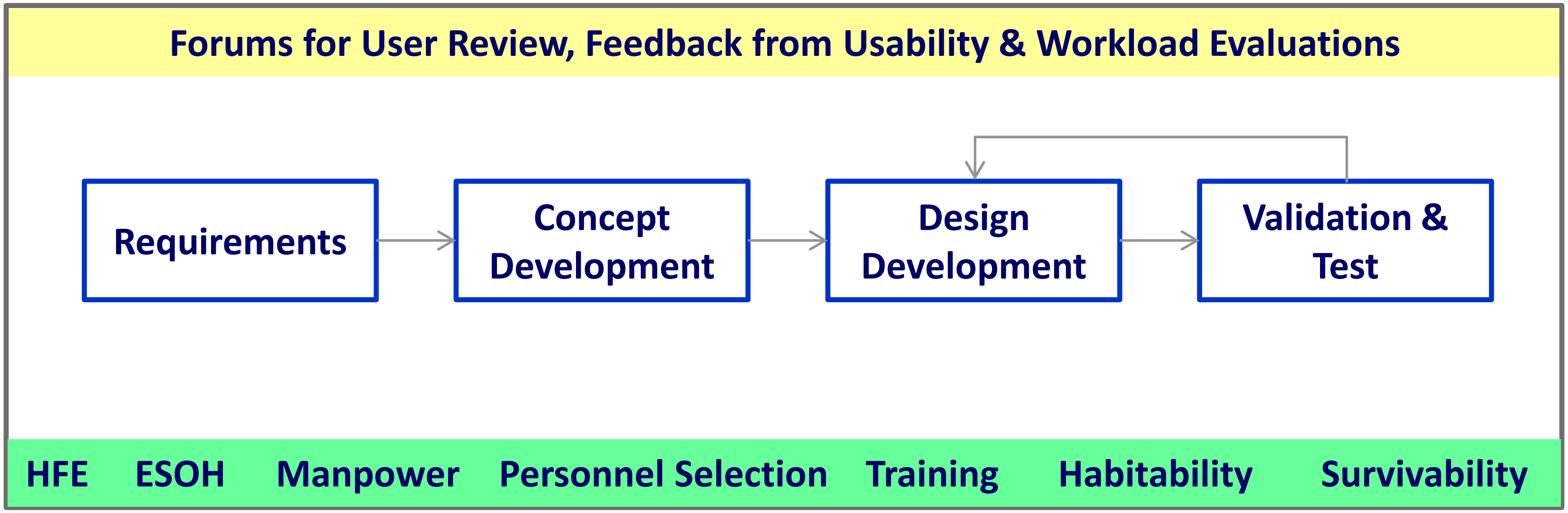
The setup: *1971, Soyuz module experiences rapid decompression event upon separation from Salyut space station.*
- Explosive bolts to separate module from station damage the pressure valve on hatch, preventing closure

-No alerts; fog formed in cabin and physiological impairment began. Crew spent precious seconds troubleshooting. Valve handle too small and required too many turns.

The Outcome: *Soyuz landed precisely. Cosmonauts were dead and could not be revived.*

Incident	Date	Mission	Fatalities	Description
Crew Exposed to the vacuum of space	June 1971	Soyuz 11	Cosmonauts- Georgi Dobrovolski Viktor Patsayev Vladislav Volkov	The crew of Soyuz 11 was killed after undocking form space station Salyut 1 after a 3-week stay. A valve on their spacecraft had accidentally opened when the service module separated, which was only discovered when the module was opened by the recovery team. Technically, the only fatalities in space above 100 km (Wikipedia)

HSI Design Process (Notional)



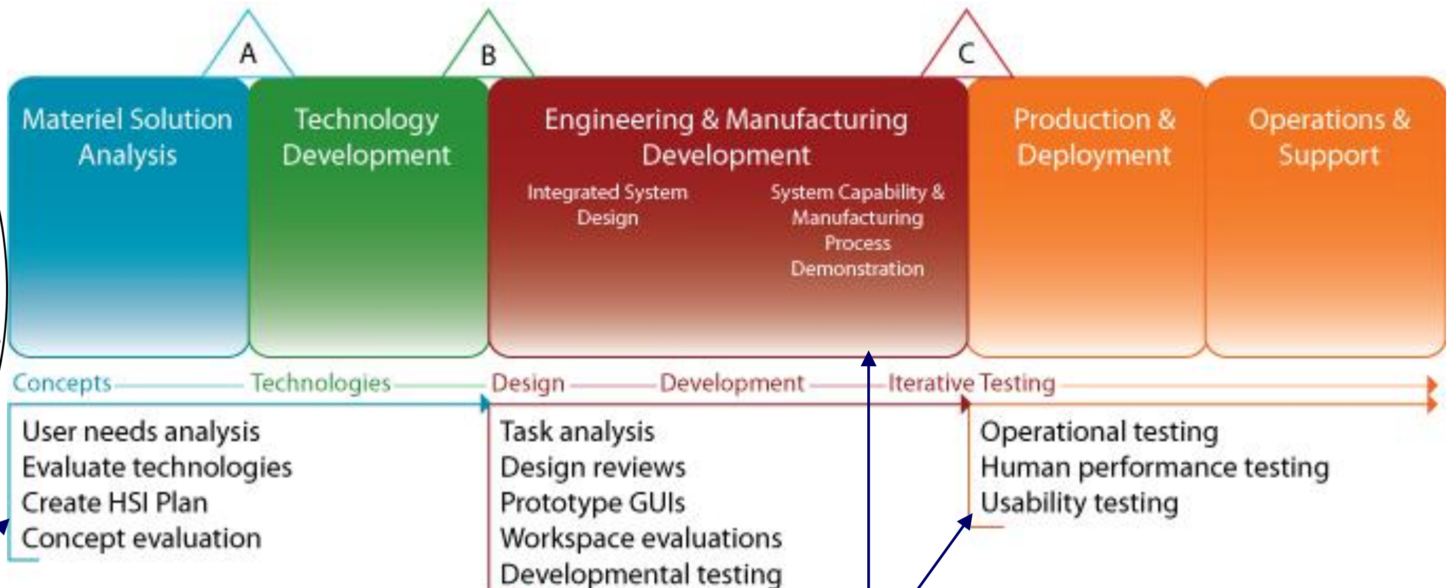
Where do Considerations for Resilient HSI Design Occur?

Acquisition Life Cycle Impact

Resiliency Supporting Activities
- changes to functional allocation/tasks
- changes to architecture, software and operator control
- changes to usability/workload study plans

MDD

System Resiliency Considerations



HSI Considerations for Resiliency
- adequate program scope
- adequate language in RFP
- adequate assessment of HSI requirements

Test
Re-allocate
Repeat
--Done

Summary & Wrap Up

- Designing in Resiliency to complex systems has many advantages
  - promotes safety, reliability and survivability of product and human operators
  - clarifies SA of who is in charge
  - optimizes manpower & staffing needs to reduce LCC
- Rephrasing the statement to ask ‘what is right about this system’ is a more constructive way to look at reliability, given that more events go right than fail
- Commitment to resiliency must be established pre-MSA, and built-in to every ConOps, RFP, Statement of Work, EMD and Test phase.
- Architectures and Software Automation designs must be flexible
- HSI and other supporting disciplines (ie; software, mission assurance, test) must be appropriately scoped, staffed and funded to achieve ‘malleable function allocation’ which may resemble re-design.
  - how do you know when you’re done?
  - does resiliency work with modification efforts that rely on COTs/NDI equipment?
- Find a way to consider resiliency in rapidly fielded systems
  - Are these synergistic or opposing goals?

Contact

For questions or follow-up, please contact:

Elaine M. Thorpe
Technical Fellow, Human Systems Technology
The Boeing Company
Huntington Beach, CA
(714) 896-3800
elaine.m.thorpe@boeing.com