

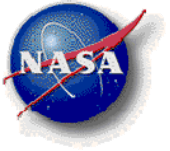
Some Safety Considerations in NextGen

Amy Pritchett

NASA Aviation Safety Program Director

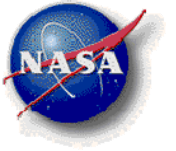
May 6th, 2008

One NextGen Goal: Safer Aircraft



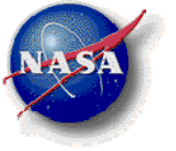
- Aircraft Aging and Durability
- Integrated Resilient Aircraft Control
 - Better understanding of upset conditions
 - Adaptive control and guidance of aircraft
 - Damaged/failed aircraft
 - Aircraft outside normal flight envelope
- Integrated Vehicle Health Management
 - On-board detection, diagnosis, prognosis and mitigation
 - Structures, propulsion, electronics, software
 - Off-line data mining

A Related Goal: Safer Aircraft Operations



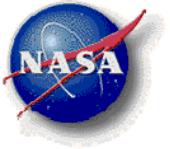
- Intelligent Integrated Flight Deck
 - Sensing of external hazards
 - Designing to support human performance
 - Automation
 - Information management and display
 - Design methods and tools

Are Humans the Problem or the Solution?



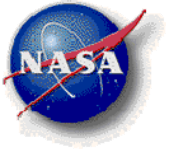
- Sometimes we make the humans sound like the problem... “the problem with the current system is that it is human-centric” ...
- Can anyone name an accident not caused by ‘human error’?
- We don’t even systematically record all the cases where humans ‘saved the day’ – that’s their job

Do We Understand the Human Contribution?



- Let's run a simulation of the NAS in which every human follows procedures exactly – what will be the result?
 - Emergency (unforeseen) conditions
 - Off-nominal (foreseen but outside envelope)
 - Nominal
- Corollary: We don't have the knowledge to automate the current system
- Corollary: Risk needs to be purposefully distributed between technology, procedures and human performance

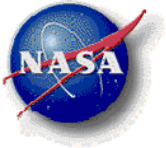
What Should Be the Human Contribution in Next Gen?



- Is it wise to plan for:
 - Automated activity beyond the capability of the human
 - Human supervising the automation for automation failures
 - Human intervening in degraded operations beyond the design limits of the automation

???

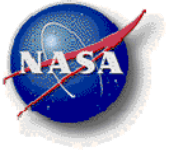
What Should Be the Human Contribution in Next Gen?



These are not new questions – concerns raised at a 1963 autoland conference

- *“A conclusion seems to follow from the above comments. If a suitable means is not provided to the pilot to enable him to land the airplane, then a suitable means should be provided to prevent the pilot from interfering with the automation during the last critical phase... It follows therefore that, if the full authority is left to the pilot, the actual reliability level is just that of the pilot himself with the information he has got, irrespective of the possible much higher reliability level of the black boxes – and the aircraft.” (Bartoli, 1963)*
- *“[We] have been striving ... [to] retain the preponderance of the control in the hands of the captain and his crew not only in favor of their dignity but also in favor of overall safety... We would like to see the Autoland used as the autopilot is used during cruise, that is to say as an aid and a contribution to rest rather than a new pain in the neck.” (Turcat, 1963)*

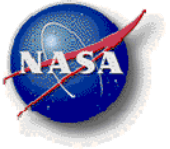
But we don't need to take this to the human 'versus' automation extreme!



How Can Human & Automation Work Together?

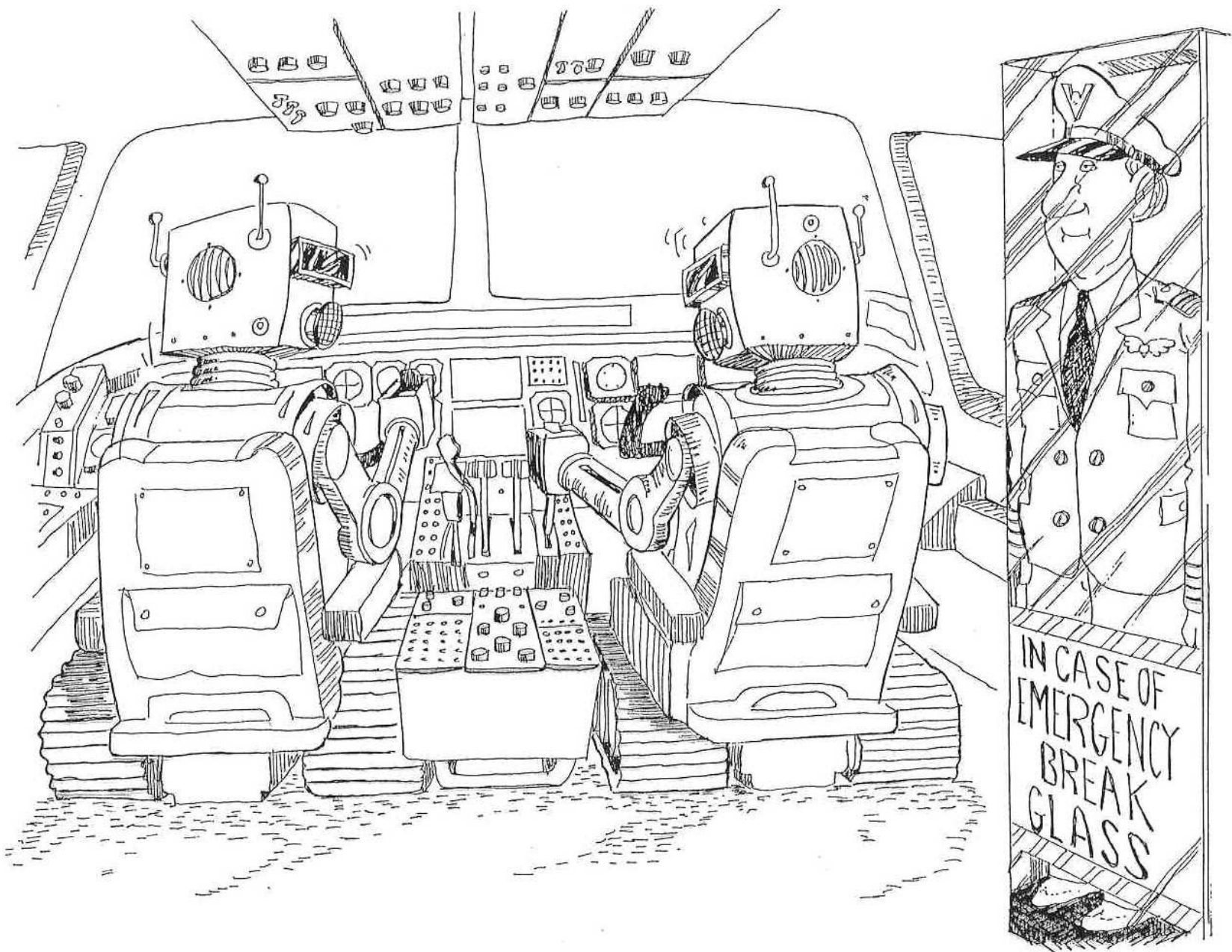
- Viewpoint of a 'joint cognitive system'
 - If the machine is smart, think of the '(happily-married) spouse metaphor' rather than the 'machine metaphor'
 - Needs to design machine functionality from the start so that it can work fluidly within a human team
- Keep the focus on the work they achieve together – not the machine's functioning
 - Human will know what work they would like to see happen
 - If the relationship between work and machine functions is clear, then the interaction is 'intuitive'

Describing Automation



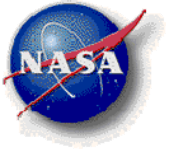
- Robustness: The range of operating conditions with satisfactory performance
- Autonomy:
 - (Engineering): The sophistication of the automation's behaviors when objective and subjective reality overlap – regardless of problems with robustness
 - (Management): The ability to go do any task, no matter how simple, and report back when the manager should know anything

Robustness will be our bigger challenge!



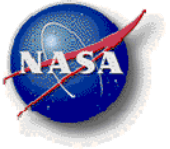
IN CASE OF
EMERGENCY
BREAK
GLASS

Adaptive Systems



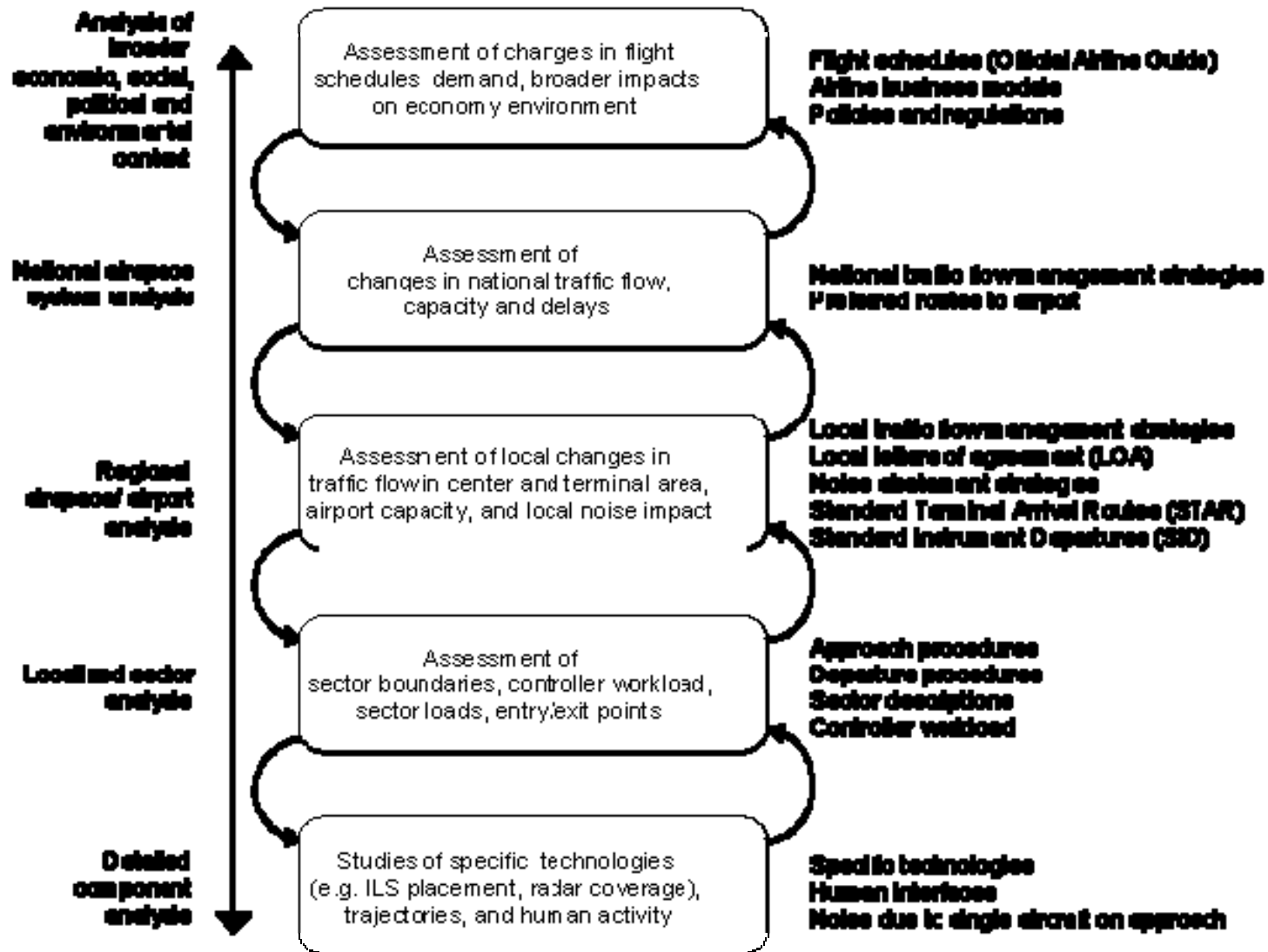
- What if we want a system that can adapt to conditions outside the (nominal) flight envelope?
 - We can't describe *a priori* its behavior
- Maybe we would need to ask different questions:
 - “Is it possible for the adaptive system to cause harm?”
 - “Can the adaptive element recover from a failure in adaptation?”
 - “Is there a way to verify the adaptation function (in flight test) without risk to the vehicle?”

Emergence

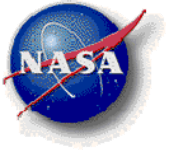


- Emergence: Behaviors observed at one level of abstraction which can not be predicted (maybe not explained!) at a different level of abstraction
- Example:
 - An unstable compression wave in a traffic stream in which each aircraft is individually stable
- My hypothesis: Many aspects of complex system safety are emergent phenomenon
 - How does analysis at one level extrapolate to another?

Many Possible Abstractions!

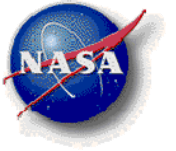


Safety: Friend or Foe?



- Addressed early, many improvements to safety can also help capacity (and vice versa)
- Left to late, safety may become the biggest programmatic risk in the implementation of NextGen

Thank You!



Questions?