Towards designing graceful degradation into trajectory based operations:

A human-machine systems integration approach

Dr. Tamsyn Edwards and Dr. Paul Lee
Agenda

• Research motivation
• Literature review: Aims
• Framework of graceful degradation
• Literature review: Detailed findings
• The operational envelope?
• Conclusions & Implications
• Next steps
Research motivation

• Trajectory based operations (TBO) is an instrumental concept in the NextGen initiative

• In order for the TBO concept to be realized, there will be a “fundamental shift in ATM” (FAA, 2014):
  – Narrower tolerances (FAA, 2014)
  – More precise trajectories
  – Strategic vs tactical

• System resilience is critical
  – TBO system must be able to gracefully degrade to maintain safe operations

• Knowledge of the causes and mitigations of degradation in TBO must be understood
Literature review

• Aims:
  – Identify causes of degradation in ATC and associated solutions
  – Identify the role of ATCOs in a gracefully degrading system
  – Develop a framework of graceful degradation from the literature

• Expected outcomes
  – Identify causes of degradation and associated solutions applicable to TBO
  – Identify literature gaps and inform future research
  – Implications for ecologically valid understanding of graceful degradation of TBO systems
Framework of graceful degradation

Degradation cause
- System fault or failure
- Environment events
- Human Operator (Air traffic controller)

Identification

Prevention and mitigation of degradation:
- Preventative measures to generate graceful degradation
- Active at different stages

System design e.g.
- Fault tolerance
- Redundancy
- Automation

Environment e.g.
- Airspace design
- Traffic flows
- CONOPS
- Procedures

Human Operator e.g.
- Training
- Human-centered interface design
- Decision support tools

Post-degradation: Recovery
- Predominantly human operator
  - Can be supported by all previous pre-degradation measures

Output

Graceful degradation
Causes: System fault/failure

• Widest range of literature
• Primarily focuses on CNS
  – Failure can be full system or partial, such as specific algorithms
• Several categorizations documented, although no consistent agreement
• Causes of hardware failure
  – Physical damage
  – Aging
  – Accidental/malicious interference
• Software failure
  – Modelling errors
  – Integration of independent ATC software
    • Legacy technology and new technology
    • Technology with competing goals
Causes: Off-nominals

• **Airspace design**
  – Number and type of conflict points
  – Size of available airspace
  – Complexity can increase ATCO demand, which may put performance at greater risk

• **Imprecision/uncertainty**

• **Off nominal events**
  – Aircraft emergencies
  – Medical emergencies
  – Unexpected pilot actions

• **Weather**
  – Widely researched
  – Leading cause of aircraft delay
  – Weather avoidance routes are pre-planned but real time updates limited
  – Consequences include manual vectoring, re-routing, delay and cancellations
  – Controllers responsible for maintaining safe operations during these demanding situations
Causes: Human operators (ATCOs)

• Least researched in graceful degradation domain
  – Human error literature in Human Factors domain

• Human performance influencing factors
  – Task demand and high workload
  – Attention and perception errors
  – Communication errors
  – Procedural error

• Human performance influencing factors resulting from use of automation (human-system interaction)
  – Underload
  – Trust
  – Design of automation – transparency and reliability
Identification

• Required prior to prevention or mitigation
• Techniques can be separated into:
  – Identifying potential causes prior to degradation
  – Identifying causes during live operations
• Techniques prior to degradation include:
  – Incident and accident analysis
  – Causal modelling
• Techniques of identification during live operations include:
  – System self-monitoring and self-identification
  – System communication to human operator
  – Human operator
Achieving graceful degradation: System-related solutions

- Well-documented in the literature
- Bertish et al. (2013) - 18 identified mitigations
  - 14/18 related to technology design and regulation
- Hardware/software solutions
  - Failure paths
  - Back up systems
  - Redundancy
- Requirements-based solutions
  - Quality standards
  - Verification and validation
- Technological solutions for environmental and human causes of degradation
  - Decision support systems
  - Automation
  - Tools to reduce uncertainty, such as enhanced weather prediction
Achieving graceful degradation: Environmental solutions

- Literature primarily focuses on reducing complexity for ATCOs
- Solutions are usually complex
- Airspace redesign
  - Standard traffic flows
  - Flight follow features
  - More efficient reroutes
  - Reduction in complexity – reduction of risk of human error
- Solutions to reduce uncertainty
  - CONOPS
  - Procedures
Achieving graceful degradation: Controller

• Contribution of ATCO to graceful degradation is under-researched
• ATCOs maintain safe operations through a high standard of performance
• Dominant contribution post-degradation—recovery
  – Role is an on-line defense between safe and unsafe operations
• Significant implications for TBO
  – System fault/failure when ATCOs are controlling more aircraft than they could without automation?
  – Framework supports breakdown of this issue
• Need for human—systems integration to support graceful degradation in TBO
  – When do ATCOs reach safe limits of performance?
The operational envelope

Normal operations:
ATC is working effectively within this workload and scenario space

At edges, due to difficulty, complexity, overload etc., performance/safety may be temporarily compromised; but situation normally recovered before loss of separation event

Here a loss of separation will occur
The operational envelope

Normal operations: ATC is working effectively within this workload and scenario space.

At edges, due to difficulty, complexity, overload etc., performance/safety may be temporarily compromised; but situation normally recovered before loss of separation event.

Here a loss of separation will occur.

Individual envelopes that interact to determine the overall system envelope.

Tolerance

System

Environment

ATCO

Operational maximum

Operational optimum
Conclusions & Implications

• Findings
  – Causes of degradation and solutions categorized by systems, environment and human operators (ATCOs)
  – Solutions to degradation can be applied pre- or post-degradation
  – Most research on systems, least on role of the ATCO
  – Research dominantly considers ATCO to be responsible for maintenance of safe operations during degradation
  – No consideration in current literature of interactions between causes and solutions

• Development of graceful degradation framework can be used to:
  – Identify research gaps
  – Identify causes of degradation and solutions
  – Identify interactions
  – Guide requirements for future research

• Human-system interaction approach essential to achieve graceful degradation in TBO
• Need to understand limits of system performance AND human performance
Next Steps

- Literature review completed
  - Paper submitted and accepted to Aviation 2017
- Aims of future work
  Identify causes of degradation in TBO
  Identify the limits of recovery for the human operator

Cognitive walk-through

- Down selection of assumptions
- Selection of use cases
- Initial understanding of recovery strategies
- Initial understanding of limits of recovery

Human in the loop simulations

- Identification of human envelope ‘limits’
- Investigation of human and system performance envelope interaction
- Development of solutions to specific TBO issue to create graceful degradation

Future goal

- Propose potential re-design of the system, airspace, or human tasks/procedures
- Monitoring the situation prior to full breakdown
- Support the recovery phase

Re-design of the system
Thank you!

tamsyn.e.edwards@nasa.gov