ASSESSING HUMAN-SYSTEM RESILIENCE POTENTIAL THROUGHOUT THE DEVELOPMENT LIFECYCLE*

Amy L. Alexander
MIT Lincoln Laboratory (MIT LL)
Lexington, MA USA
Dan Herschler
Federal Aviation Administration (FAA)
Washington DC, USA

We worked with subject matter experts to create a human-system resilience checklist that can be utilized during Independent Operational Assessments (IOAs) of air traffic control systems as part of the system acquisition process. The checklist focuses on four key areas for evaluating human-system resilience characteristics: procedures, system use, workload, and training. A resilience scoring method indicates areas where a human-machine system under consideration does or does not have resilient characteristics. Overall resilience scores can be compared among design alternatives, or across different points in system development for a particular design. The ultimate intent is to provide guidance and metrics that will enable the FAA to address human-system resilience aspects in the implementation of NextGen capabilities in the National Airspace System (NAS). The goal of increased resilience is to reduce the risks and potential impacts of disruptive events, and to safeguard the efficiency, safety, and cost effectiveness of NextGen NAS operations.

The Federal Aviation Administration's NextGen program uses many complex systems and technologies to increase the efficiency, safety, and cost effectiveness of the National Airspace System. Although NextGen systems are designed to achieve defined system availability requirements, system degradation and failure are still a very real, if remote, possibility. Designing and assessing systems with resilience to failures in mind can reduce the risks or potential impacts of degradations. Looking to the literature, there are a variety of definitions of resilience (see Reason, 2000; Sheridan, 2008); however, a number of common characteristics emerge relating to anticipating adverse effects, withstanding unexpected conditions, maintaining control, sustaining operations, and recovering quickly when something goes wrong. Resilience is defined by the FAA as maintaining safety and a minimum level of service in reaction to system failures or degradations (FAA, 2016). The underlying goal is to prevent or mitigate impacts on air traffic operations.

Previous work (e.g., Hollnagel, Woods, & Leveson, 2006) has identified characteristics of resilient organizations and human-machine systems, and initial experimental methods for assessing resilience potential have been developed. However, these methods primarily apply to existing or well-prototyped systems. In an effort to assess the resilience potential of an

---

This material is based upon work supported by the Federal Aviation Administration under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Federal Aviation Administration.

operational capability earlier in the system development lifecycle, we worked with subject matter experts to create a human-system resilience checklist that can be utilized during Independent Operational Assessments (IOAs) of FAA air traffic control systems as part of the system acquisition process. The checklist focused on four key areas, identified through collaboration with subject matter experts in conjunction with review of the resilience literature, that should be considered when evaluating human-system resilience characteristics: procedures, system use, workload, and training. A resilience scoring method was developed to provide an indication of areas where a system under consideration does or does not have resilient characteristics. The overall resilience score can then be compared to design alternatives, or across different points in the system development lifecycle for that particular design and operational context. The checklist and scoring system has yet to be validated, but upcoming IOA testing is anticipated to provide insight and feedback about the utility of this approach for assessing human-system resilience.

Method

The first step in creating the human-system resilience checklist was to identify resilient characteristics of NextGen systems, including ways to build, enhance, and assess the resilience of complex human-machine systems. MIT LL conducted a literature review on characteristics of resilient systems, particularly focused on human-automation systems (Yenson et al., 2015). System reliability, system predictability, and operator engagement emerged as three key areas for examining resilience potential. The identified characteristics of resilient automation systems were then translated into a list of phrases (e.g., a resilient system is able to handle "unknown unknown" situations). These phrases formed the basis of a resilience job aid that was originally developed in reference to the safety risk management (SRM) process, without a specific target application or end user group. An excerpt from this job aid is presented in Figure 1. The job aid specifically pointed out questions to ask and actions to take, provided detailed explanations and rationales, references to SRM documentation, and included a basic scoring method for assessing resilience potential.

	Guidance	Phase/ Document	Reference	Scoring
	risk.			
8.	For this human-machine system, what are indicators of successful system performance? Of degraded system performance? Of a failed system? Can these indicators be specified by certain measurable qualities? Such qualities and indicators can be used in combinations as indicators of human-machine system resilience. Do the metrics appropriately measure system recovery and performance levels after adverse events?	PSP, IIA	4.2.2	☐ 0: System resilience metrics not identified ☐ 1: System resilience metrics identified ☐ 2: System resilience metrics identified and considered appropriate
	Rationale: To determine if the system is resilient, practitioners should identify metrics that indicate the system's ability to adapt to, react to, and learn from abnormal conditions. These metrics can be found by selecting events or other indicators of degraded performance, such as a hazardous weather event, and monitoring a performance metric, such as throughput, before and after the event to determine how well performance returns after an event.			
9.	What are the minimum performance levels for the resilience metrics? (e.g. < 3 minutes to return to an acceptance rate of 25 aircraft per minute after an event)	PSP, IIA	4.2.2	☐ 0: Baseline metric values not set ☐ 1: Baseline metric values set
	Rationale: To determine if the system is resilient, practitioners need to set a baseline for the nominal acceptable level of performance for each of the selected resilience metrics so that later performance data can be compared against the required performance.			

Figure 1. Original Resilience Job Aid Excerpt

Various discussions regarding resilience with the FAA led us to the Independent Safety Assessment Team (AJI-321) of the FAA Air Traffic Organization's (ATO) Safety and Technical Training office, which is responsible for conducting independent operational assessments (IOAs) of designated NextGen systems. IOAs verify new FAA systems or solutions are suitable, operationally effective, and safe prior to deployment in the NAS. Specifically:

- IOAs are independent from the FAA office responsible for deploying the new system/capability.
- IOAs are conducted at operational key sites during live NAS operations.
- IOAs are major structured assessments with the purpose of identifying safety hazards and operational concerns with new systems/capabilities.

AJI-321 agreed for IOA to be a focus area for our work, and we coordinated across seven working group meetings to review the original resilience job aid and customize it for use during IOAs. We determined that a more streamlined checklist would be most appropriate for the IOA context. Working group meetings then focused on carefully reviewing the overall checklist content, categorizing questions in a meaningful way, and revising the wording of the questions and their associated responses. Usability and usefulness of the checklist as well as a resilience scoring system were also discussed as our checklist development progressed.

Checklist

The final checklist contained questions broken down into four key categories for evaluating human-system resilience characteristics: procedures, system use, workload, and training. Example questions from each checklist section are presented in Figures 2-5. Questions were presented with up to four response options, each having a point value associated with it as well as a color-coded indicator of goodness (red: not indicative of a resilient system, yellow: resiliency needs improvement; green: indicative of a resilient system). The evaluator was instructed to select the most appropriate response for each question, and there were comment fields for any additional notes that would be helpful to capture.

4. Are detailed and appropriate <u>procedures</u> available for a wide range of situations, including:	See sub-question responses below:			
a. System usage under nominal conditions?	0: No	1: Yes, but most procedures need to be improved	2: Yes, but some procedures need to be improved	3: Yes
b. The most frequent and/or critical known off-nominal events?	0: No	1: Yes, but most procedures need to be improved	2: Yes, but some procedures need to be improved	3: Yes
c. Assessing system recovery and performance levels after adverse events?	0: No	1: Yes, but most procedures need to be improved	2: Yes, but some procedures need to be improved	3: Yes
d. Bringing the system down and back online for maintenance?	0: No	1: Yes, but most procedures need to be improved	2: Yes, but some procedures need to be improved	3: Yes
e. Certification of systems?	0: No	1: Yes, but most procedures need to be improved	2: Yes, but some procedures need to be improved	3: Yes
Comments:				

Figure 2. Example Procedures Checklist Questions

9. Does the system notify the controller if a degradation occurs?	0: No	1: For some critical functions	2: For most critical functions	3: For all functions
Comments:				
10. Are there design aspects within the system (e.g., alerts, warnings) that safeguard against controller errors and adverse conditions?	0: No	1: For some critical functions	2: For most critical functions	3: For all functions
Comments:				

Figure 3. Example System Use Checklist Questions

24. What types of tasks are performed by the controller under steady-state (i.e., nominal) conditions?	0: Tasks involve more passive monitoring than intended	0: Tasks involve more active engagement than intended	2: Tasks are the appropriate passive/active mix
Comments:			
25. Under steady-state conditions, does the system allow for an appropriate controller workload level?	0: Workload is too low – controller is disengaged	0: Workload is too high – controller is overloaded	2: Workload is appropriate
Comments:			

Figure 4. Example Workload Checklist Questions

33. Which of the following are provided as part of the human-machine system training protocol?	See sub-question responses below:			
a. Minimum training requirements?	0: Not addressed	1: Yes, but requirements need to be greatly improved	2: Yes, but requirements need to be somewhat improved	3: Yes, addressed adequately
b. Training on system vulnerabilities?	0: Not addressed	1: Yes, but training needs to be greatly improved	2: Yes, but training needs to be somewhat improved	3: Yes, addressed adequately
c. Operational aids (e.g., cheat sheet, help line) for less-experienced users?	0: Not addressed	1: Yes, but aids need to be greatly improved	2: Yes, but aids need to be somewhat improved	3: Yes, addressed adequately
d. Training sessions on contingency procedures?	0: Not addressed	1: Yes, but training needs to be greatly improved	2: Yes, but training needs to be somewhat improved	3: Yes, addressed adequately
e. Training sessions on novel events?	0: Not addressed	1: Yes, but training needs to be greatly improved	2: Yes, but training needs to be somewhat improved	3: Yes, addressed adequately
Comments:				

Figure 5. Example Training Checklist Questions

Checklist Scoring

A basic scoring system was developed to tally across responses and provide an ordinal resilence score for each of the four categories. An example resilience scorecard for the procedures category is presented in Figure 6. Total points possible are broken into three levels to provide a general assessment of low/moderate/high human-system resilience. Individual category scores can then be combined to provide an overall human-system resilience score, as shown in Figure 7.

Procedure Resilience Scorecard

Question	Response Score	Max Score Possible (Benchmark)
1.		3
2.		3
3a.		3
3b.		3
4a.		3
4b.		3
4c.		3
4d.		3
4e.		3
5.		1
6.		1
Total		29

0 – 9: Low Procedure Resilience
10 – 19: Moderate Procedure Resilience
20 – 29: High Procedure Resilience

Figure 6. Procedure Resilience Scorecard

Overall Resilience Scorecard

Category	Category Score	Max Score Possible (Benchmark)
Procedures		29
System Use		37
Workload		20
Training		47
Other (Q40)		1
Total		134

0 – 44: Low Resilience
45 – 89: Moderate Resilience
90 – 134: High Resilience

Figure 7. Overall Resilience Scorecard

This simple scoring system was developed so as not to imply any unwarranted precision in quantifying certain responses or categories over others. The notion here is that the checklist provides an indication of areas where a system under consideration does or does not have resilient characteristics, and a basis of comparison among design alternatives, or across different points in system development for a particular design, to determine if the design of a system is improving over time from a resilience perspective.

Conclusions

In an effort to assess the resilience potential of a system, we worked with subject matter experts to create a human-system resilience checklist that can be utilized during IOAs of air traffic control systems as part of the system acquisition process. The checklist and scoring method presented here have yet to be validated, but application of the revised checklist during upcoming IOA testing may provide initial validation and feedback about the utility of the checklist approach for assessing human-system resilience.

Acknowledgements

This material is based upon work supported by the Federal Aviation Administration under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Government or the Federal Aviation Administration.

References

Federal Aviation Administration (2016). *Performance Based Navigation NAS Navigation Strategy 2016.* US Department of Transportation.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience Engineering: Concepts and Precepts*. Aldershot, UK: Ashgate, 2006.

Reason, J. (2000). Reducing human error through safety management practices. Presented at *The 14th Annual FAA/CAA/Transport Canada Human Factors in Aviation Maintenance Symposium*. Vancouver, Canada. Retrieved from: http://www.faa.gov/about/initiatives/maintenance_hf/library/documents/media/mx_faa_(formerly_hfskyway)/strategic_program_plan_(1998)/14th_symposium/reducing_human_error_through_safety_management_practices.pdf

Sheridan, T. (2008) Risk, human error, and system resilience: Fundamental ideas. *Human Factors, 50,* 418-426. doi: 10.1518/001872008X250773

Yenson, S. K., Phillips, S., Davis, A., & Won, J. (2015). Exploring human-system resilience in air traffic management technologies. Presented at the *2015 IEEE/AIAA 34th Digital Avionics Systems Conference*. DASC. doi: 10.1109/DASC.2015.7311403