Research, Engineering Development Advisory Committee
Subcommittee on Aircraft Safety (SAS)

Meeting Summary:

The Subcommittee on Aircraft Safety (SAS) met on September 6 and 7, 2017 in Atlantic City, NJ, at the FAA William J Hughes Technical Center, for its routine fall meeting. This meeting had three specific objectives on its agenda:

1. Review and provide comment on the FAA's 2017 safety research plan accomplishments and ongoing research.
2. At FAA leadership and REDAC request, review and provide comment on the FAA's recently released Cyber Security Plan.
3. Deep dive into continued significant topics of UAS, General Aviation Safety and Fatigue management.

To assess the 2017 research plan performance, SAS continued to utilize our new portfolio review approach developed for our last meeting. Rather than the traditional quad charts we have historically reviewed the FAA staff prepared a Research Program Area Review. This review bundled current and proposed research into 15 major program areas. We then had an opportunity to gain a higher-level insight into the research tasks and performance against planned research deliverables in 2017. Additionally, we were provided visibility to more comprehensive funding information which enabled a broader picture of the research efforts. All SAS members agreed that this method of review, while still not perfect, was far superior to prior efforts and that the Subcommittee dialogue was greatly enhanced. Findings and Recommendations resulting from these discussions and related to general aviation safety, fatigue management and UAS are attached to this report.

In advance of the meeting the FAA's recently completed cyber security plan was distributed for committee review. The committee was presented a summary of this plan during the meeting and detailed discussion with the plan's authors resulted. A high-level summary of committee comments is attached to this report. Detailed comments have been provided directly to the plans authors.

SAS continued its practice of engaging both Subcommittee members and agency expertise to inform our discussions. At this meeting presentations from MITRE, Boeing and Honeywell informed our views on the future directions of industry. Additionally, we were provided with a briefing on AVS certification reform. This was a beneficial briefing as many of our research findings and recommendations are certification support based.

The SAS will meet next on March 14 and 15, 2018 in Washington, DC. We hope to be able to dedicate some time with the AVS management team to ensure continued alignment with REDAC and AVS leadership objectives.

Respectfully Submitted,
Ken Hylander
Chair, REDAC Subcommittee on Aviation Safety

Research, Engineering Development Advisory Committee
Subcommittee on Aircraft Safety (SAS)

2017 Fall Meeting Findings and Recommendations

UAS Findings and Recommendations

The SAS greatly appreciated the initial presentation on the FAA UAS R&D Plan and commends the FAA's efforts. The plan is a comprehensive identification of research required to meet the different UAS implementation phases and the research being performed by FAA, other government agencies, industry and academia. While we have not yet had the opportunity to review the plan itself, we understand that it identifies gaps in ongoing and planned research and required funding to cover the next 5 years. The FAA is to be commended for undertaking such an ambitious planning activity. We look forward to the opportunity to review the entire plan once it is released.

Finding 1

A significant portion of the FAA's research budget is being directed to the UAS COE. From the FAA's description, it appears that the majority of UAS research is in the form of university grants (i.e. the majority of the research is conducted by the UAS COE). Grants tend to be less driven by specific outputs and thus potentially less directed towards a specific practical aim or objectives of the applied research needs identified in the FAA UAS R&D plan. The subcommittee wonders whether the FAA is receiving full value from such research given the magnitude of the applied research identified in the plan.

Recommendation 1

The FAA should steer grants towards more goal directed research and should consider taking advantage of a contract vehicle to conduct more applied research at the UAS COE aimed at meeting the applied research objectives to identified in the FAA UAS R&D Plan.

Finding 2

The subcommittee noted that peer-reviewed UAS Ground Collision Severity Evaluation research is not being fully leveraged by AFS-800 in granting Part 107 waivers for UAS operations over people. A clear and closed loop connection between the research performers and the consumer of the research results appears to be lacking. The subcommittee senses that research results are not taken into sufficient consideration in UAS safety oversight, rulemaking and other actions required for achieving UAS integration into the NAS.

Recommendation 2

Through all stages of research activities, there should be tighter engagement among research performers and the FAA organization(s) that would leverage research results in safety oversight activities and rulemaking. FAA should consider how to best utilize existing structure to assure the maximum transfer of research learning.

Finding 3

The plan identifies a significant amount of required research and FAA indicated that there will likely be insufficient funds to conduct all of the research identified in the necessary timeframe.

Recommendation 3

The subcommittee recommends that FAA, together with its stakeholders, identify the minimum acceptable research results required to achieve each transition step and revise the plan accordingly. The FAA, together with its stakeholders should prioritize the research.

Finding 4

The advanced research that is ongoing to allow UAS to safely and efficiently integrate into the NAS can, in some cases, provide safety and efficiency benefits in the manned sector. While clearly there is direct applicability to highly automated manned aviation such as with the burgeoning "on-demand mobility" concept vehicles, this research can also inform more traditional forms of manned aviation including airline transportation segments. An example of this might be allowing the crew to take advantage of see and avoid concepts that might keep the aircraft a farther distance from large birds or other airborne conflicts.

Recommendation 4

The UAS research should place added emphasis on communicating research findings which can provide parallel benefits within the unmanned and manned aviation sectors.

Fatigue Mitigation and Research Finding and Recommendation

Finding 5

The committee received a follow-on briefing on the FAA's overall fatigue research program. The committee feels that this report described the existence of a wide-ranging fatigue research program within the FAA, and a strong interest in building follow-up research documenting the effectiveness of the FRMS/FRMP. The report identified an effective plan for moving forward which involved among other things, identifying research initiatives from around the industry, gaps in knowledge, and the establishment of fatigue working group with members from industry, research, and regulators to continue the necessary follow-up work needed to ensure required research is performed. The report stated that this working group will need a sponsor from the regulatory community to provide guidance and tasking for the working group.

Recommendation 5

The FAA establish a Fatigue Working group, identify an FAA working group lead who will best represent fatigue across the agency, execute the FAA plan that was presented as the path forward for identifying and addressing fatigue research issues, and properly implementing the research results. Follow-up studies of the effectiveness, utility, and potentially necessary enhancements of the FRMS/FRMP should be funded and implemented as soon as possible.

Research, Engineering Development Advisory Committee
Subcommittee on Aircraft Safety (SAS)

Comments on the FAA's Cyber Security Research Plan

REDAC SAS is happy that the FAA has developed a cyber security plan because as we become increasingly dependent upon software-intensive systems for the safe and efficient operation of aviation system, the attack surfaces are multiplying. We have non-homogenous complex interconnected systems that have vulnerabilities at the seams. This risk has been identified as an emerging issue for several years.

Listed below is a summary of REDAC SAS thoughts on the FAA's Cyber Security Research Plan. These are only high-level comments. Detailed specific comments on the plan have been already been provided separately to the plan authors.

1. Several REDAC sub-committees (or perhaps REDAC itself) should consider enhancing their committee membership to include cyber expertise. These threats will infiltrate many aspects of the FAA domains. It is difficult to assess the research plans and provide comprehensive thought without the appropriate levels of expertise engaged.
2. More clearly define the plan's scope to include aircraft systems. The introductory material and overall plan description do not seem to match the contents of the plan. Much of the introductory material talks about protecting FAA systems and infrastructure with little mention of aircraft and other non-FAA critical aviation cyber systems. Section 1.0 talks about the information systems that the FAA operates but never mentions that the FAA has safety oversight responsibility of information systems which are components of aircraft, airlines, and airports. Much of the research addresses this role, but the introductory material seems to ignore. This was only alluded to with the statement "…participate in the protection of the aviation sector as a whole…"
3. FAA should fully leverage the ongoing work of DoD, and others, in this area in order to accelerate the pace of progress. The timelines in this plan appear too slow for this rapidly evolving threat.
4. The industry collaborations seem weak and should be strengthened as part of the overall plan.
5. There is an entirely new human skill set that will be needed in future workforces to address ongoing cyber threats which goes beyond Human-in-the-Loop detection and responding. We believe that some research related to developing a workforce with specialized skills that can stay one step ahead is essential.
6. Heed the ARAC Tasking Group recommendations (ASISP Working Group final report section 5.3)
7. This plan captures the on-going work and identifies some research needs that appears to be unfunded (because there is no funding or products identified in the plan). The plan does not make it clear what needs are unfunded. We think it is appropriate to identify needs that are not currently funded.
8. Several of the plan research outcomes are weak. They mostly take the form of "provide insights…" and "provide a basis for rulemaking…". These need to be strengthened – what specifically will be the impact/value and how will it be measured!
9. We believe that there are several needed areas of research missing from the plan including:
    a. **Commercial space:** There is no identified need to develop cybersecurity guidance for commercial spacecraft. This an emerging area that should be identified. This should cover all mission stages, from design and development of spacecraft and payload systems, launch, on-orbit operations, and end-of-life.

b. **Potential for changes in UAS rules and use cases:** The R&D plan seems limited to use cases currently allowed under FAA rules (e.g., UAS line of sight ops, etc). A good R&D plan should explore potential opportunities and challenges of expanded or modified rules. The plan should explicitly state they will explore the application of advancing technologies such as artificial intelligence and machine learning (e.g., in autopilots), 5G cellular, laser communications, etc., and resulting cybersecurity implications under various use cases.
c. **Accident investigation.** No mention is made of inclusion of cyber causes or factors in accidents, or technologies to aid in identification of a cyber-attack as the cause of a mishap or accident. We suggest inclusion of research at all layers (i.e., the aircraft systems, but also in the ATC/NAS), into how additional data can be collected, stored, and analyzed to: 1) identify whether a mishap was cyber-related; 2) attribute the attack to a nation or individual; 3) isolate the vulnerability or vulnerabilities to a subsystem, software module, or manufacturer so that the vulnerability may be mitigated.
d. **Threat characterization.** Guidance should be given to aircraft and avionics manufacturers, as well as to airlines and other operators, on the types of cyber threats, potential impact, and probability of occurrence. This ties to quantitative risk management. In addition to simply exploring vulnerabilities, research is needed to prioritize threats and provide guidance to industry on what they are expected to address, and what could be considered outside of their responsibility
e. **Test and Evaluation / Certification**. The plan does not include any reference to development of technologies to assess the effectiveness of cybersecurity capabilities by operators or manufacturers. The FAA should be able to provide guidance to proponents on testing/assessment techniques. R&D should be done to determine how cyber defenses can be tested for non-IT systems such as aircraft. This would enable FAA to author appropriate guidelines, policies, etc.