Federal Aviation Administration

AVS Research, Engineering and Development

AVS RE&D Portfolio:

Digital System Safety (A11Ds)

Research Plan: 2022- 2027

January 26, 2022

Part 1: BLI Definition and Scope

Program Area: Digital System Safety (A11Ds)

FAA Domain: Digital Systems and Technology

BLI Scope: Digital System Safety (A11Ds)

Aircraft PNT Cyber Safety: GPS and FAA's WAAS transmit unencrypted, unauthenticated digital data messages. Open public standards and products enable spoofing. What once required expensive military assets is now achievable using legal, hobby-grade devices and software. These avionics are essentially networked computers and the antennas are unsecured entry ports for potential threats—comparable to an internet connection with no firewall or virus protection. These research projects address specific DOT tasks assigned in *U.S. Space-Based Positioning, Navigation, and Timing Policy (Space Policy Directive 7,* the *National Implementation Plan signed by OST-R in May 2021,* and the Aug 2021 OSTP *National Research and Development Plan for Positioning, Navigation and Time Resilience* to pursue GPS and WAAS authentication and advanced antenna technologies to enable resilient and responsible use such that disruption or manipulation does not undermine aviation safety or national economic security.

This research enables the assessment of FAA requirements and technical capabilities to enable avionics processing of authenticated WAAS and GPS services. Planned activities are in collaboration with the FAA WAAS Program Office, DOT OST-R, and AF Research Laboratory as providers of the authenticated signals and data messages, and with aviation industry representatives developing a new generation of resilient avionics.

Aircraft Software, Programmable Hardware, Artificial Intelligence and Machine Learning based systems provide tremendous flexibility and power to express how aircraft systems should behave using these technologies. This permits us to add functionality that would be impossible without these technologies, but faults in design and implementation using these technologies can be difficult to eliminate and be disastrous if present. Due to the growth in size and complexity of these systems, our traditional development and verification approaches may reach a point when we are unable trust them. These "soft" technologies are already forcing us to choose between deployment and risks. The diversity of future systems will need new guidance to ensure growth can continue without compromising safety. A research program is needed to understand how industry and regulators can establish confidence in flying vehicles in the presence of rapid technological developments.

Part 2: Service/Office Research Requirements and Research Gap Analysis

1.0 Operational Capability: WAAS/Satellite Based Augmentation System (SBAS) Avionics Authentication

Definition: Preclude aircraft or pilot inadvertent use of manipulated and synthesized "false" GPS and WAAS/SBAS signals and data messages from unsophisticated, national policy acknowledged threat devices that are perceived by the aircraft and pilot as valid signals and data with potentially catastrophic results in the absence of appropriate mitigations.

Primary S/O: AIR-602, AIR-622
Secondary S/O: AJM-3 Navigation Services

S/O Priority: 1

Outcome: Validation of FAA Technical Standard Order avionics requirements for SBAS authentication, GPS authentication, and advanced antenna consistent with U.S. aviation interests.

Research Gap Analysis

Research Questions	Contribution	Research Output
1.1 What GPS and SBAS cryptographic and advanced antenna TSO requirements can avionics incorporate to address nationally acknowledged GNSS disruption and manipulation (spoofing) threats to enable resilient aircraft operations consistent with 2021 executive order and national policy directed tasks, OSTP national research plan objectives, and DOT OST-R implementation plans for execution of the national policy direction?	100%	Validation of SBAS authentication, GPS authentication, and advanced antenna TSO requirements and aircraft integration guidance to enable resilient and responsible use of GNSS services consistent with U.S. aviation interests.

2.0 Operational Capability: Software Assurance based Certification

Definition: The ability to accept non-prescriptive based evidence that permits approval of a wide range of aviation vehicles that use digital technologies and perform in diverse environments.

Primary S/O: George Romanski, AIR-600
Secondary S/O: N/A

S/O Priority: 2

Outcome: The current practice of showing that the software of a safety related system can be trusted is based on objectives defined in current guidance documents, DO-178 and others. The techniques proposed are based on software methodologies that were popular 40 years ago, with minor updates to the core document with some additions through supplemental documents.

A clearer understanding is must be developed to support the acceptance of digital systems in safety related environments. The risks of software induced faults and their distribution in a growing software base must be better understood so that they can be mitigated. Research into the effectiveness of alternatives to the prescriptive approaches using software maturity, and system resilience will result in more affordable development and acceptance processes.

Research Gap Analysis

Research Questions	Contribution	Research Output
2.1 Does the a non-prescriptive certification approach provide an effective means of showing that software for lower level risk systems is acceptably safe?	30%	Develop an understanding the residual risks in Software developed for systems at a lower criticality levels and approaches to mitigating these risks using non-prescriptive approaches to be developed and evaluated. A balance between risks and effort should be defined and documented.
2.2 Are architectural means available to lower the costs of deployment of safety related systems without compromising safety?	30%	As processing power, memory and hardware integration capabilities continue to drop in price, the ability to build systems out of many separate elements becomes easier. Develop a description of the possible approaches that would permit such systems and describe how they could still be shown to satisfy their safety properties.
2.3 How can the safety continuum be mapped on a certification continuum more closely and result in more effective deployment and acceptance?	40%	The current approach of categorizing risks and development approaches using identifiers does not provide a continuous evaluation mechanism. Develop a new mechanism to map these properties on a continuous scale.

3.0 Operational Capability: Approval of AI/ML Based Systems

Definition: Approval of Artificial Intelligence and Machine Learning based systems requires the development of evidence that the system is trained to performs its intended function safely and evidence exists to show that it can be trusted.

Primary S/O: George, Romanski, AIR-600
Secondary S/O: N/A

S/O Priority: 3

Outcome: A description of the approaches that could be used by applicants and authorities to confirm a level of trust in an AI/ML based control system that supports automation.

Research Gap Analysis		
Research Questions	**Contribution**	**Research Output**
3.1 Given that machine learning data-set is always incomplete compared to the operational data set, how would a system balance the needs of generalization and rigor.	25%	Develop a means of balancing the needs of generalization with operational rigor as objectives that could be used to assess the safety of an AI/ML aviation product.
3.2 The initial deployment of AI/ML based systems are likely to be low criticality advisory-based systems. How can this be scaled up in practice?	25%	Develop recommendations for the use of learning systems that can evolve and establish confidence through use, without labeling all input/output training sets.
3.3 The AI/ML learning process uses huge amounts of computing power and memory that is often outsourced. How can these be constrained, configured and saved so that the trust in their use is established and preserved.	25%	Document how cloud based development for AI/ML can be used and document objectives that should be established to establish a level of trust in the results.
3.4 In traditional software development all of the steps all of the transformation steps can be explained if necessary, so they are understood. Can the transformations in an AI/ML system be explained to a sufficient level of understanding so that trust in the final system will emerge.	25%	Develop a means of explaining the steps a system takes during training and deployment that yield an explainable description of the operational AI/ML based system.

Part 3: RE&D Management Team Programming

BLI Planning 3 Year Funding Profile (FY22-24) as of 01/28/2022

YEAR	Appropriation or Formulation Contract Funding ($)	INITIAL BLI TEAM PLANNING CONTRACT FUNDING – AFN BLI Target minus the Hold Back ($)	AVS-1 APPROVED CONTRACT FUNDING ($)
FY22 formulation or appropriation (if known)	**$1,760,526**		
FY23 formulation	**$3,217,556**		
FY24 AFN funding allocation target		**$1,738,058**	**$4,825,000**

BLI Plan 5 Year Outlook (FY22-27)

Complete (C)	In Progress (IP)	Programmed (P)	Need (N)

Research Activities	FY22	FY23	FY24	FY25	FY26	FY27
Operational Capability 1.0: Aircraft PNT Cyber Safety						
1.1 Preclude aircraft or pilot inadvertent use of manipulated and synthesized "false" GPS and WAAS/SBAS signals and data messages from unsophisticated, national policy acknowledged threat devices that are perceived by the aircraft and pilot as valid signals and data with potentially catastrophic results in the absence of appropriate mitigations.	*IP*	*P*	*N*	*N*	*N*	*N*
Research Activities	**FY22**	**FY23**	**FY24**	**FY25**	**FY26**	**FY27**
Operational Capability 2.0: *Software Assurance based Certification*						
2.1 Does the non-prescriptive certification approach provide an effective means of showing that software for lower level risk systems is acceptably safe?				*N*	*N*	
2.2 Are architectural means available to lower the costs of deployment of safety related systems without compromising safety?				*N*	*N*	
2.3 How can the safety continuum be mapped on a certification continuum more closely and result in more effective deployment and acceptance? 6			*P*	*N*		
Research Activities	**FY22**	**FY23**	**FY24**	**FY25**	**FY26**	**FY27**
Operational Capability 3.0: *Approval of AI/ML Based Systems*						
3.1 Given that machine learning data-set is always incomplete compared to the operational data set, how would a system balance the needs of generalization and rigor?			*P*	*N*		

3.2 The initial deployment of AI/ML based systems are likely to be low criticality advisory-based systems. How can this be scaled up in practice?				*N*	*N*	
3.3 The AI/ML learning process uses huge amounts of computing power and memory that is often outsourced. How can these be constrained, configured and saved so that the trust in their use is established and preserved?				*N*	*N*	
3.4 In traditional software development all of the steps all of the transformation steps can be explained if necessary, so they are understood. Can the transformations in an AI/ML system be explained to a sufficient level of understanding so that trust in the final system will emerge?			*P*	*N*		

Part 4: BLI Team Members

Participants Name	Role	Routing Symbol
Jorge Fernandez	BLI Chair	AIR - 670
Ken Alexander	CSTA/Sponsor SME	AIR-600
George Romanski	CSTA/Sponsor SME	AIR-600
Srini Mandalapu	Performer SME	ANG-271
Michael Welch	Performer SME	ANG-C31