

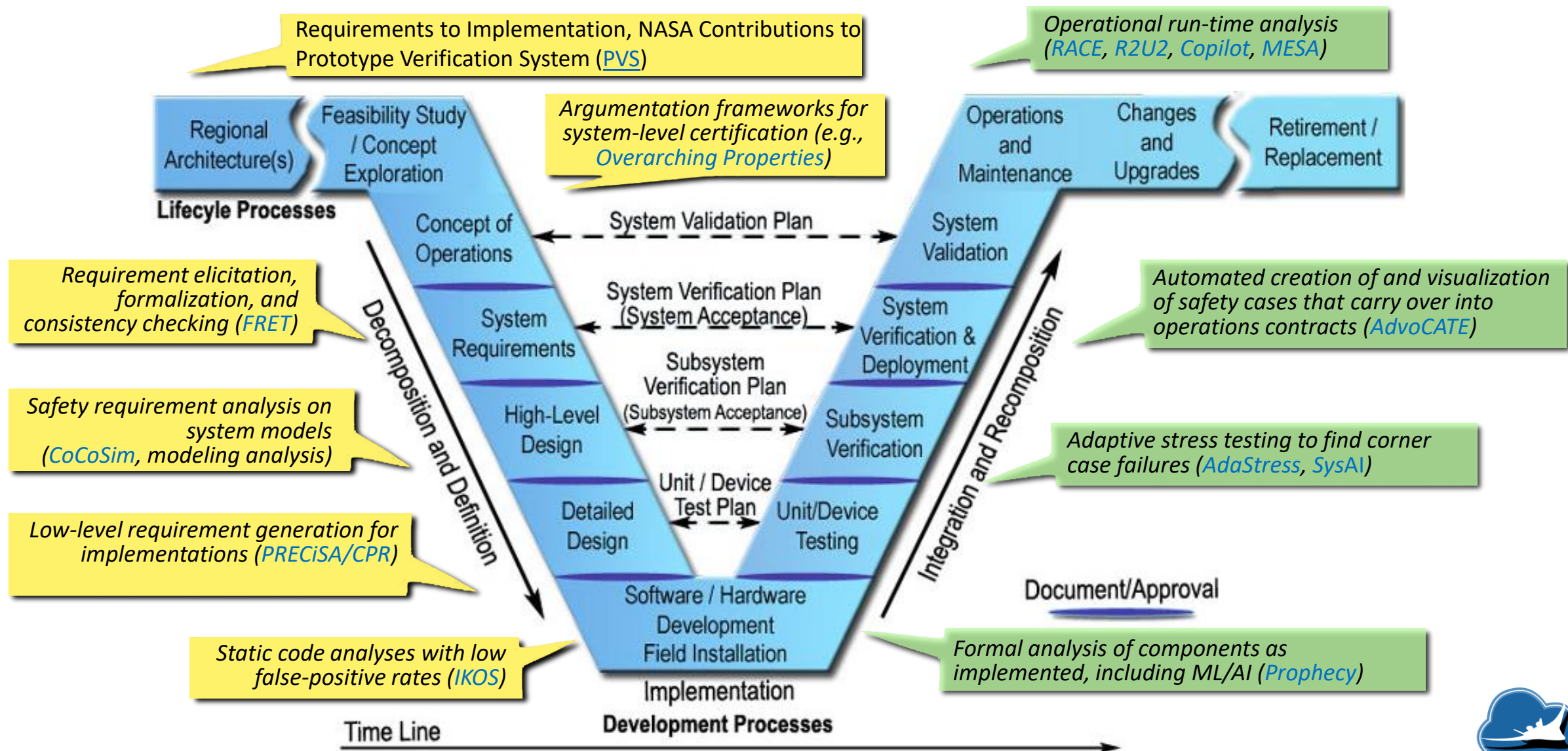
Meeting Objectives



- **Close out the Critical Commitment for System Wide Safety's Technical Challenge 3 (TC-3)**
Deliver validated methods and recommended practices to reduce certification costs for ground and on-board vehicle guidance and control systems through expanded acceptability of analysis as evidence for certification FY 2022.
- Communicate results to maximize public awareness of the research and transfer capabilities via a set of *on-demand training seminars* and supporting materials including *reports, publications and open source software codes* where applicable.



Capabilities Span the Entire Design Cycle



On-Demand Training Seminars (10)



1. **AdaSTRESS**: Software package that implements the Adaptive Stress Testing (AST) framework, which determines the likeliest failures for a system under test.
2. **AdvoCATE**: Automate the creation, manipulation, and management of large-scale safety assurance cases based on a formal theory of argument structures.
3. **CoCoSim**: CoCoSim (Contract based Compositional verification of Simulink models) is used to verify user-supplied requirements.
4. **Copilot**: A realtime programming language and Runtime Verification framework that allows users to write concise programs in a simple but powerful way using a stream-based approach.
5. **CPR**: Compact Position Reporting Algorithm is a set of functions defined to Aviation Standards that encode and decode aircraft positions. CPR* is a formally verified C implementation of CPR's functions that use computer arithmetic in fixed- and floating-point formats.
6. **FRET**: Formal Requirements Elicitation Tool is a framework for the elicitation, formalization and understanding of requirements.
7. **IKOS**: IKOS (Inference Kernel for Open Static Analyzers) is a static analyzer for C/C++ based on the theory of Abstract Interpretation.
8. **Overarching Properties**: An International effort to develop a minimum set of properties sufficient for use in the approval process.
9. **PRECiSA**: Program Round-off Error Certifier via Static Analysis) is a fully automatic analyzer for the estimation of round-off errors of floating-point valued functional expressions.
10. **SysAI**: (System Analysis using Statistical AI), which is a flexible statistical learning framework for V&V and analysis of complex and high-dimensional Aerospace systems with AI components.



Additional Capabilities (Without Seminars)



NASA Lead:

1. **AMASE**: Architectural Modeling and Analysis for Safety Engineering
2. **Case Studies** for DO-330 and DO-333
3. **Fmdtools**: Fault Model Design tools is a toolkit for modelling system resilience in the early design phase.
4. **MESA**: MESSage-based System Analysis is a framework that provides runtime verification of distributed systems in a nonintrusive manner.
5. **MIKA**: Manager for Intelligent Knowledge Access is an assistive knowledge manager for decision support and formulating recommendations in the In-Time Aviation Safety Management System (IASMS).
6. **Prophecy**: Property Inference for Deep Neural Networks
7. **R2U2**: R2U2 (Realizable, Responsive, Unobtrusive Unit) is a hardware-supported tool and framework for the real-time system and software health management of cyber-physical system
8. **RACE**: The Runtime for Airspace Concept Evaluation (RACE) is a software architectures and framework to build configurable, highly concurrent and distributed message based systems.

NASA Contributed to:

1. **SAVI PVS**: System Architecture Virtual Integration contributions to the System Architecture Virtual Integration Program (SAVI)
2. **SAVI**: System Architecture Virtual Integration Program (SAVI)
3. **SOTERIA**: An automated way to synthesize safety-informed architectures



Suggested NASA Online Resources



Organizations

Programmatic

- Aeronautics Research <https://www.nasa.gov/aeroresearch>
- Airspace Operations and Safety Program (AOSP) <https://www.nasa.gov/aeroresearch/programs/aosp>
- System-Wide Safety (SWS) Project <https://www.nasa.gov/aeroresearch/programs/aosp/sws>

Technical

- Formal Methods Research Program <https://shemesh.larc.nasa.gov/fm/>
- Robust Software Engineering <https://www.nasa.gov/isd-robust-software-engineering>

NASA technical documents, images and etc.

- *NASA Technical Reports Server (NTRS)* provides access to NASA metadata records including conference papers, journal articles, meeting papers, patents, research reports, images, movies, and technical videos – scientific and technical information (STI) created or funded by NASA. <https://ntrs.nasa.gov/>

Open source resources

- Policy: NASA uses open source to address project and mission needs, to accelerate software development, and to maximize public awareness and impact of our research.
<https://www.nasa.gov/open/open-source-development.html>
- Repositories: NASA public, open source development repositories are at [SourceForge](https://sourceforge.net/) <https://sourceforge.net/> and GitHub <https://github.com/nasa>
- Catalog of NASA Software: <https://code.nasa.gov>



Backup Slides



“The introduction of **software and digital components** has allowed the development of increasingly **complex systems** but at the same time has required changes and additions to basic engineering approaches and methodologies. Basic research in new tools and techniques is needed for designing and testing software-intensive systems and for **maintaining** and **upgrading** them over time. For example, most software cannot be exhaustively tested...

There is a need for new ways to provide assurance, particularly for critical systems.”

[Decadal Survey of Civil Aeronautics Foundation for the Future](#) (2006)

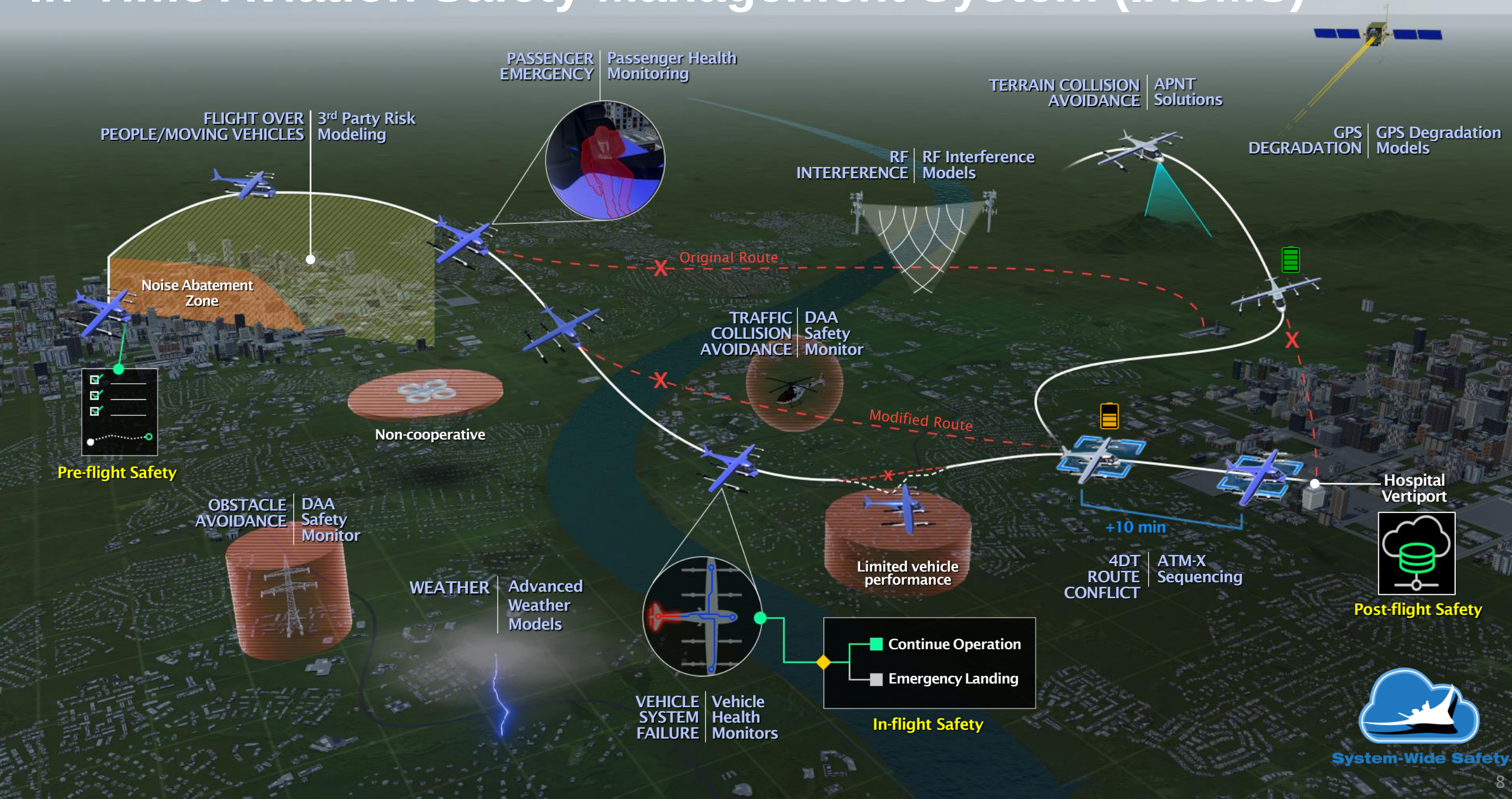
Why NASA ?

- Supporting Infrastructure
- Mission Alignment
- Lack of Alternative Sponsors

What research is ongoing?

... “[for] System Verification, Validation, and Certification. There is no accepted approach to verification and validation that leads to certification of a software system as complex as an [In-Time Aviation Safety Management System], particularly if, as expected, the system includes adaptive, nondeterministic algorithms...”. [**In-Time Aviation Safety Management: Challenges and Research for an Evolving Aviation System**](#) (2018)

In-Time Aviation Safety Management System (IASMS)

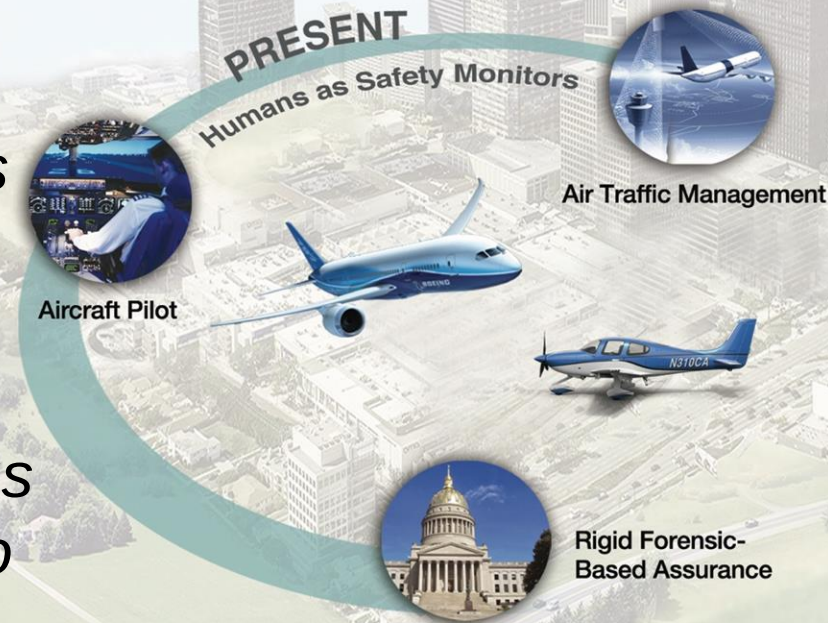


Aviation Safety—Where We Are



The high level of safety in our current system has evolved over time. Every accident or mishap triggers an investigation and often new rules.

These features that keep us safe can also be barriers to growth and novel operational concepts.



* Risks here refers to safety-related risks; which may be mitigated during operations or during design.



Aviation Safety—What Must Change



Enable a safe, transformed NAS:

- Identify the largest safety barriers
- Address the barriers that NASA is uniquely positioned to solve
- Leverage research in traditional operations to inform safety requirements for emerging operations
- Lead the emerging market community to tackle remaining key technical barriers, and
- Act as a catalyst to engage and galvanize the community around future aviation system safety requirements and research.



To maintain current levels of safety, the transformed NAS will need **different safety mechanisms and protections** than our present system.



The relationship to the big picture of SWS



“Challenge Summary Statement: There is no accepted approach to verification and validation that leads to certification of a software system as complex as an IASMS...

... for small UAS. Greater understanding is needed with respect to creating a process to certify and/or license increasingly autonomous UAS hardware, software systems, and operators. Reporting requirements for UAS operations are insufficient, and those that do exist have not been organized in coordination ... “

In-Time Aviation Safety Management: Challenges and Research for an Evolving Aviation System (2018)

“Barrier Statement: The lack of generally accepted design, implementation, and test practices for adaptive/ nondeterministic systems will impede the deployment of some advanced IA systems and aircraft in the NAS.”

National Academies of Sciences, Engineering, and Medicine. 2014. Autonomy Research for Civil Aviation: Toward a New Era of Flight. Washington, DC: The National Academies Press.

<https://doi.org/10.17226/18815>.



The relationship to the big picture of SWS



Verification, Validation, and Certification. Develop standards and processes for the verification, validation, and certification of IA systems and determine their implications for design.

Specific tasks to be carried out by this research project include the following:

- Characterize and define requirements for intelligent software and systems.

- Improve the fidelity of the VV&C test environment.

- Develop, assess, and propose new certification standards.

- Define new design requirements and methodologies for IA systems.

- Understand the impact that airspace system complexity has on IA system design and on VV&C.

- Develop VV&C methods for products created using nontraditional methodologies and technologies.**



The measured impact based on the latest NRA



- **Cost savings through automation.** These are the savings resulting from the improved efficiency due to formal methods tools for automating verification activities as compared to the traditional approach.
 - one subsystem about a 12% saving via automation of test writing. This is based on the assumption that the requirements modeling cost incurred by the domain expert is used instead of the modeling cost incurred by an experienced formal methods practitioner. If the latter is used, then a 19% saving was observed.
- **Cost savings through reduction of rework.** These are the savings resulting from the use of formal methods to identify issues that were missed by earlier iterations of traditional development processes and therefore resulted in rework.
 - Observed on average cost savings of 26% per sprint via reduction of rework for the four sprints.
- **Quality improvements.** These are issues or corner cases found but that were missed or would not have been found until later phases by the traditional development process, primarily due to the completeness of the formal analysis.
 - Insufficient evidence to claim any cost savings.

Critical Commitment Map – Near-term



Deliver validated methods and recommended practices to reduce certification costs for ground and on-board vehicle guidance and control systems through expanded acceptability of analysis as evidence for certification (Enabler for Thrust 5 and 6). FY 2022

Will fulfill critical commitment in FY2022 using evidence and documentation from the completion of TC3. Direct NASA development towards TC3 ended in 2018, and remaining work and evidence will be collected with completion of NRAs in FY22. *(Details to follow.)*

