



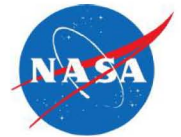
Systems-wide Safety and Assurance Technologies

SSAT Project

Robert W. Mah, Ph.D.
SSAT Project Scientist

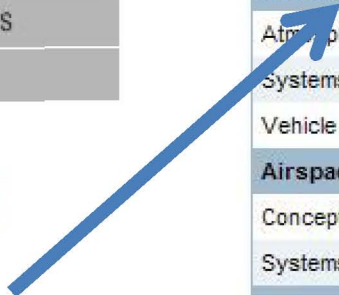
Fault Management Workshop
New Orleans
April 10, 2012

Systems-wide Safety and Assurance Technologies



- + Home
- Aeronautics Research Mission Directorate**
- + ABOUT US
- + PROGRAMS
- + ARMD NRA
- + TECHNICAL EXCELLENCE
- + PEOPLE
- + PARTNERSHIPS
- REFERENCE MATERIALS**
- + EVENTS AND EXHIBITS
- + EDUCATION
- + AERO MEDIA RELEASES
- + MULTIMEDIA

- Related Links**
- + [Project POC List](#)
 - + [ARMD RFI/NRA \(2006\)](#)



REFERENCE MATERIALS: PROJECT POC LIST

For information about the following program area thrusts, please contact the point of contact listed below. Click on the name to email your query.

Fundamental Aeronautics Program Projects	Point of Contact
Hypersonics (FA)	Jim Pittman
Supersonics (FA)	Peter Coen
Subsonics: fixed wing (FA)	Ruben DelRosario
Subsonics: rotary wing (FA)	Susan Gorton
Aviation Safety Program Projects	Point of Contact
Atmospheric Environment Safety Technologies	Renato Colantonio
Systems-wide Safety and Assurance	Ashok Srivastava
Vehicle Systems Safety Technologies	Paul Krasa
Airspace Systems Program	Point of Contact
Concepts and Technology Development	Rudy Aquilina
Systems Analysis, Integration & Evaluation	Neil O'Connor
Integrated Systems Research Program	Point of Contact
Environmentally Responsible Aviation	Fay Collier
Integration of UAS into the NAS	Chuck Johnson

SSAT Project Objective (from NASA PRG)



Objectives: The System-Wide Safety and Assurance Technologies (SSAT) project **will identify risks and provide knowledge** required to safely manage increasing complexity in the **design and operation of vehicles and the air transportation systems**, including advanced approaches to **enable improved and cost-effective verification and validation** of flight-critical systems.

The Project will address the following challenges:

- **[Develop] verification and validation tools** for manufacturers and certifiers to use to assure flight critical systems are safe in a rigorous and cost- and time-effective manner.
- **[Understand and Predict] system-wide safety** concerns of the airspace system and the vehicles by developing technologies that can utilize vehicle and system data to accurately identify precursors to potential incidents or accidents.
- **[Understand] the key parameters of human performance** which provide the human contribution to safety in aviation.
- **[Predict] the [remaining useful] life** of complex systems by reasoning under uncertainty about root causes (diagnosis) and predict faults and remaining useful life (prognosis) across multiple systems.



NASA
Aeronautics Research Mission Directorate

FY 2012 Planning, Programming,
Budgeting and Execution Process

Program and Resources Guidance

May 6, 2010

Project Reorganization



IVHM Project (2007 – 2010)



SSAT Project

System-wide safety



VSST Project

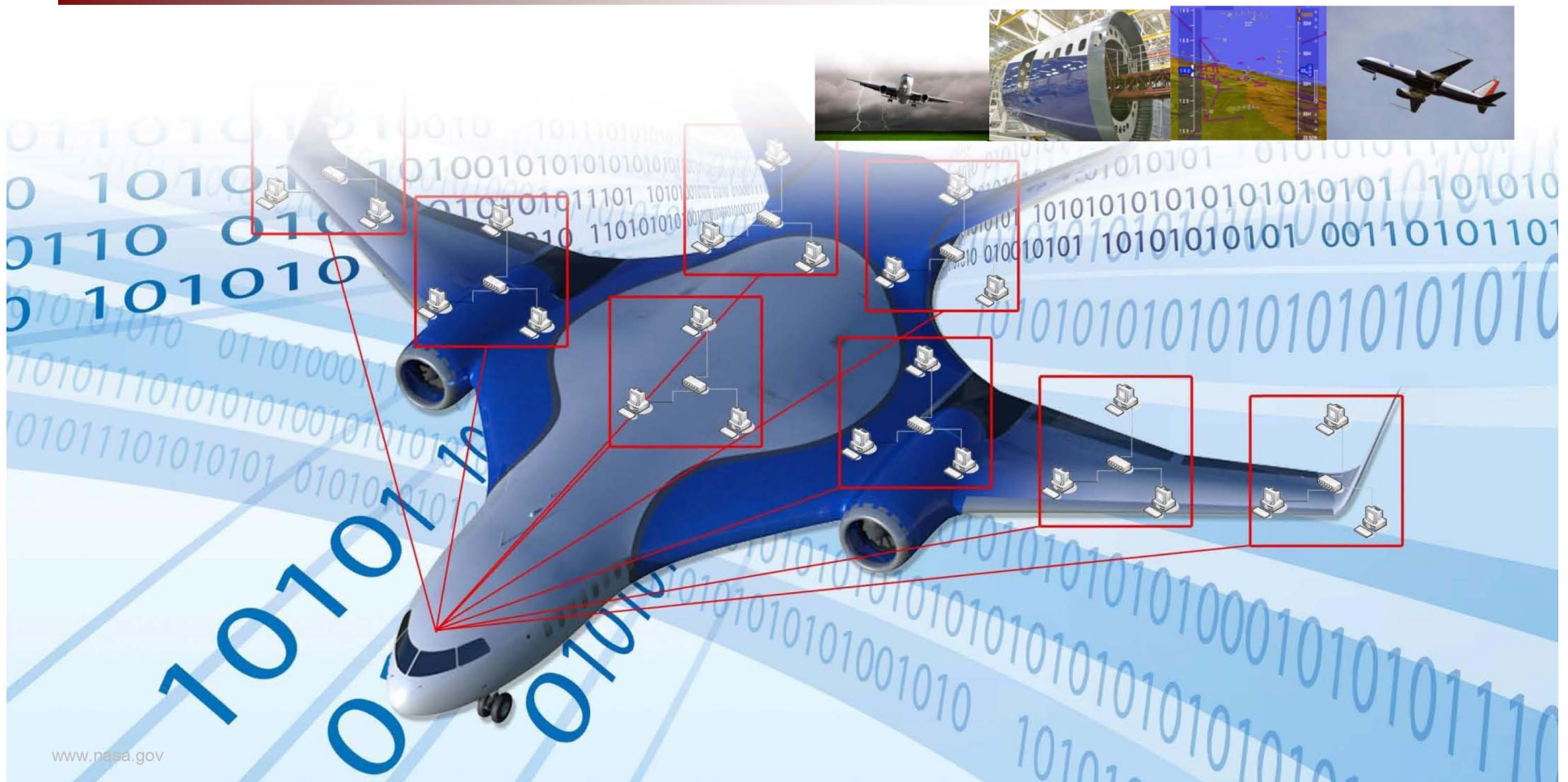
Vehicle systems safety





Aviation Safety Program Integrated Vehicle Health Management (IVHM) Project

Dr. Ashok Srivastava, Principal Investigator
Dr. Robert Mah, Project Scientist
Robert Kerczewski, Acting Project Manager



IVHM Project Goals



“Develop technologies to reduce accidents and incidents by developing vehicle health management systems to determine the state of degradation for aircraft subsystems; developing and demonstrating tools and techniques to mitigate in-flight damage, degradation, and failures”

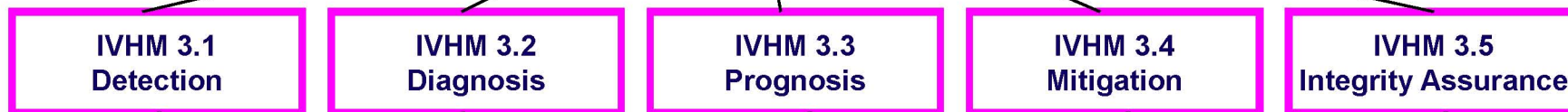
IVHM Research Framework



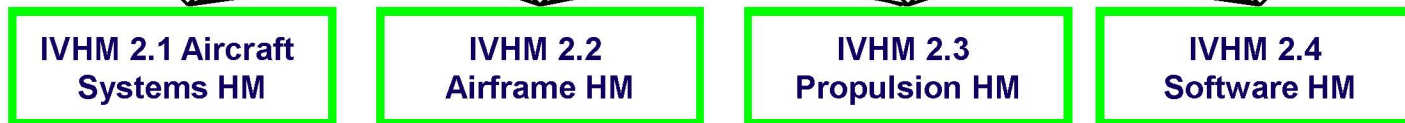
Level 4 – Aircraft Level



Level 3 – Themes



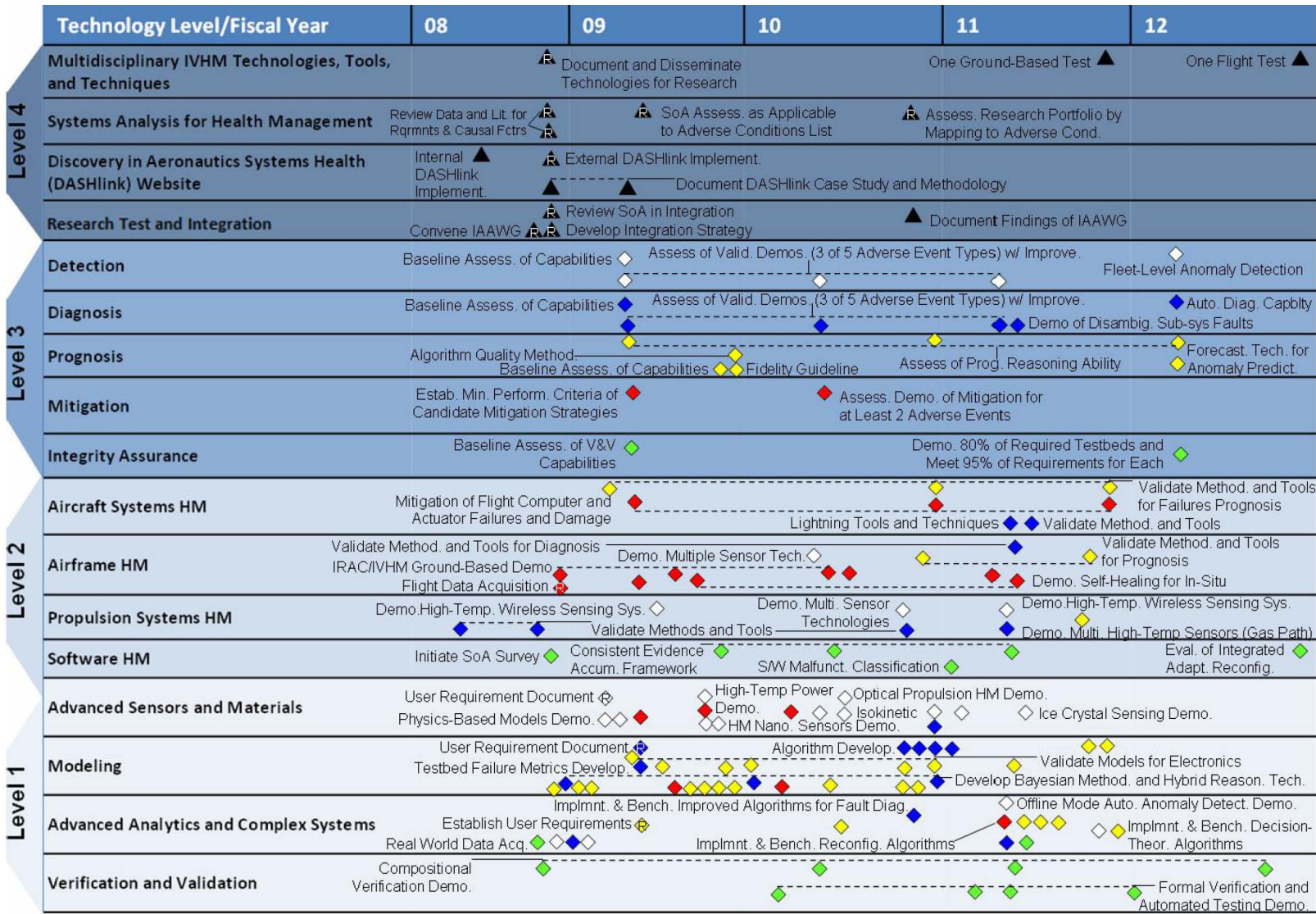
Level 2 – Subsystems



Level 1 – Foundational



IVHM Major milestones (5 year plan)



Key: Level 4 ▲
 Recurring ▲
 Detection ◇
 Diagnosis ◆
 Prognosis ◆
 Mitigation ◆
 Integrity Assurance ◆

IVHM NRA Partners



- **Our Portfolio**

- On-board system failures and faults – 3 active
- Detection -- 6 active and 1 completed in FY10
- Diagnosis -- 7 active and 1 completed in FY10
- Prognosis -- 6 active and 1 completed in FY10
- Mitigation -- 2 active
- Integrity Assurance -- 5 active
- Ongoing monitoring of operational data -- 3 active



- **Tracking Progress**

- All reviews are conducted **annually** at the Project Level: PI, PM, PS, API, COTR/TM + other interested parties
- Reviews are conducted via WebEx
- Review comments are formally collected and forwarded to awardee via COTR/TM
- Many face-to-face interactions occur annually at both NASA and awardee sites
- All NRA documentation is stored on NX so that the entire project team has access



- **NRA Value to IVHM**

- Overall the performance of the NRA awards were judged VERY GOOD.
- Each award is mapped to one or more approved IVHM Technical Plan milestones.





Validated, proactive solutions for ensuring safety in flight and operations

0
1
0
1
0
0

SSAT Project Goals



- “**Understanding and predicting system-wide safety concerns** of the airspace system ...and the vehicles as envisioned by NextGen, including the emergent effects **of increased use of automation to enhance system efficiency** and performance beyond current, human based systems, through **health monitoring of system-wide functions that are integrated** across distributed ground, air, and space systems....
- Develop fundamentally new data mining algorithms to support automated data analysis tools to integrate ... from a diverse array of data resources”

- “Research to improve **confidence and timeliness** of certification... “
- “Develop improved **system engineering processes** and tools for determining optimum roles **of humans and automation** in complex systems...”

- Applied Research on Complex Systems Validation and Verification
- Applied Research on Vulnerability Discovery
- Applied Research of Human Performance Models
- Applied Research on System Health Management

SSAT Research Framework



Level 2 – Project Level

Goal – Develop validated multidisciplinary tools and techniques to ensure system safety in NextGen to enable proactive management of safety risk through predictive methods.

SSAT 2.1 Technical Challenges

SSAT 2.2 Systems Analysis (SA)

SSAT 2.3 Partnerships and Outreach

SSAT 2.4 Research Test & Integration (RTI)

Level 3 – Subproject

SSAT 3.1
Verification &
Validation of Flight Critical
Systems (VVFCS)

SSAT 3.2
Data Mining and
Knowledge
Discovery (DMKD)

SSAT 3.3
Human Systems
Solutions (HSS)

SSAT 3.4
Prognostics and
Decision Making
(PDM)

Level 4 – Subproject Elements

- SSAT 4.1.1: Argument-Based Safety Assurance
- SSAT 4.1.2: Authority and Autonomy
- SSAT 4.1.3: Distributed Systems
- SSAT 4.1.4: Software Intensive Systems

- SSAT 4.2.1: System-Level Reasoning
- SSAT 4.2.2: Anomaly Detection from Massive Data Streams
- SSAT 4.2.3: Discovery of Causal Factors
- SSAT 4.2.4: Prediction of Adverse Events

- SSAT 4.3.1: Human Automation Tools
- SSAT 4.3.2: Operational Complexity Metrics and Methods
- SSAT 4.3.3: Human Performance Mechanisms

- SSAT 4.4.1: Decision Making under Uncertainty
- SSAT 4.4.2: Diagnostics
- SSAT 4.4.3: Prognostics
- SSAT 4.4.4: Software Health Management

“Validated, proactive solutions for ensuring safety in flight and operations”

SSAT Project Technical Challenges

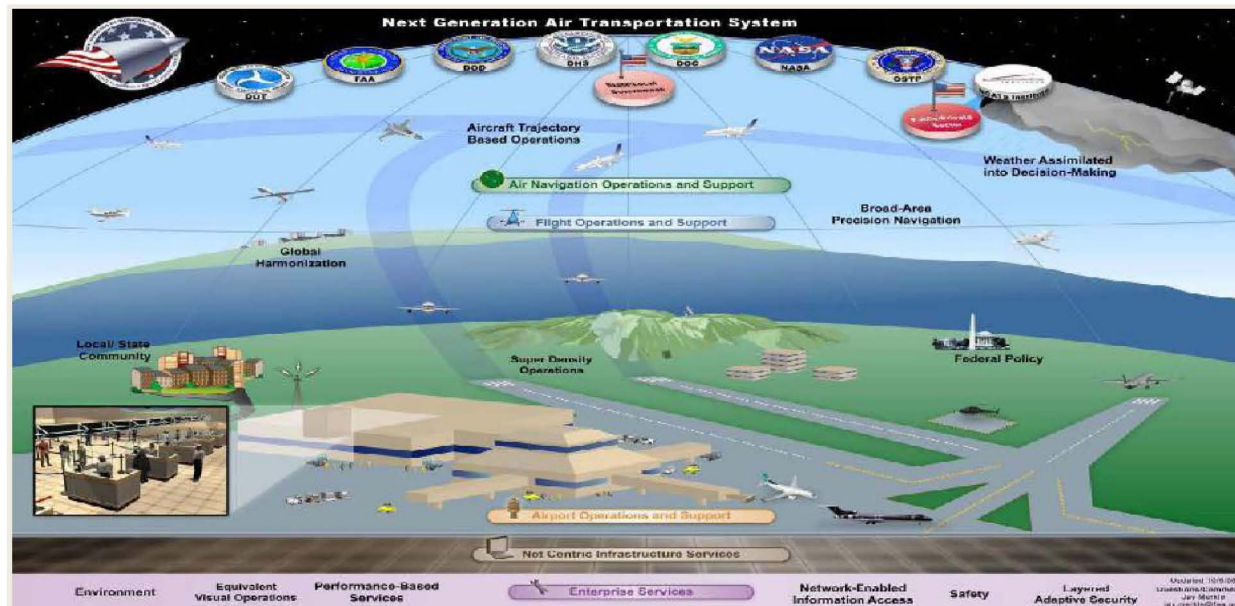


1. Assurance of Flight Critical Systems (FY25)

Development of **safe, rapid, and cost effective NextGen Systems** using a unified safety assurance process for ground based and airborne systems.

2. Discovery of Safety Incidents (FY19)

Automated discovery of previously unknown **precursors** to aviation safety incidents in **massive** (>10 TB) heterogeneous data sets.



3. Automation Design Tools (FY20)

Increase safety of human – automation interaction by incorporating **human performance considerations** throughout the design lifecycle in NextGen technologies.

4. Prognostic Algorithm Design for Safety Assurance (FY25):

Development of **verifiable** prognostic algorithms to help **remove obstacles to certification.**

Technical Challenge 1

Assurance of Flight Critical Systems

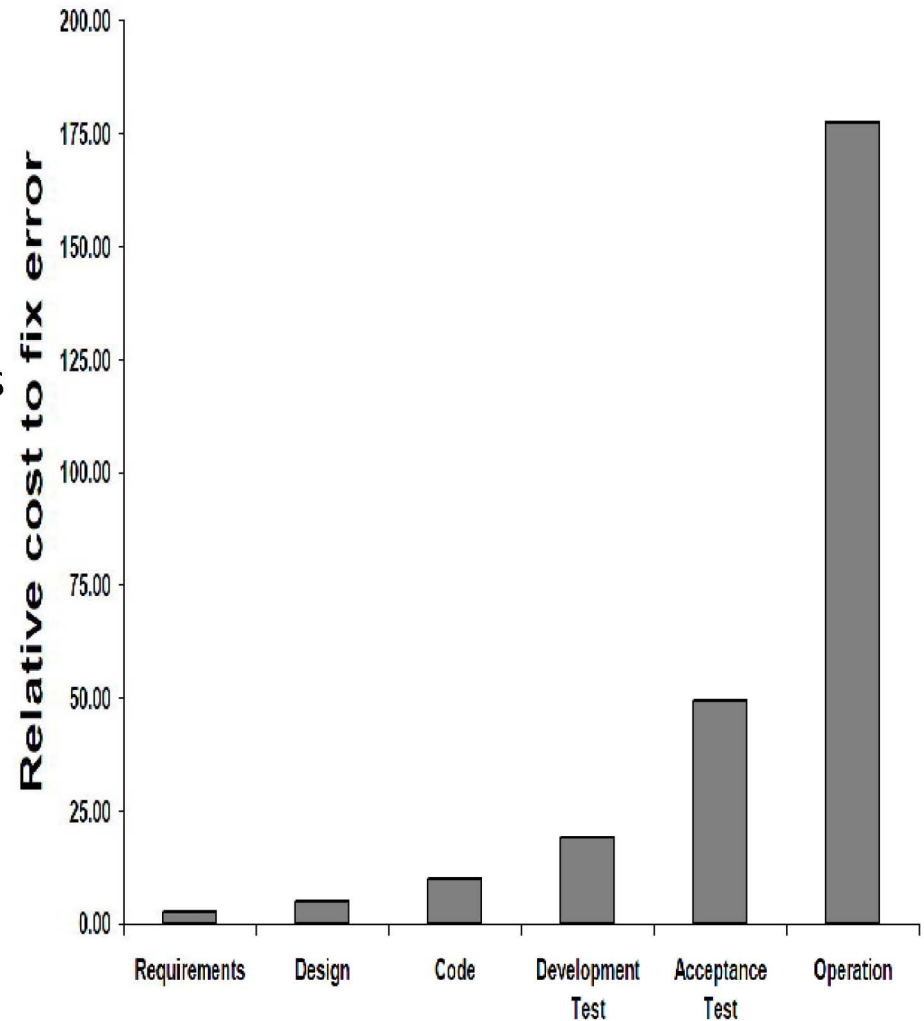


Safe and Rapid Deployment of NextGen

Fill a critical gap in the life-cycle development of complex systems for NextGen by developing **time- and cost-effective techniques** for verification and validation of complex civil aviation systems that will unify processes for ground based and airborne systems (FY25).

Benefits:

- **Rapid but safe incorporation of technological advances** in avionics, software, automation, and aircraft and airspace concepts of operation.
- Availability of safety assurance methods for **confident and reliable certification**, enabling manufacturers and users to exploit latest technological advances and operational concepts.



Phase in which error was detected and corrected

Boeing 787 software cost ~\$4.5B

Technical Challenge 2

Discovery of Safety Incidents



Automated discovery of previously unknown precursors to aviation safety incidents (FY19).

A **first-of-a-kind demonstration** of the automated discovery of precursors to aviation safety incidents through analysis of **massive heterogeneous data** sets.

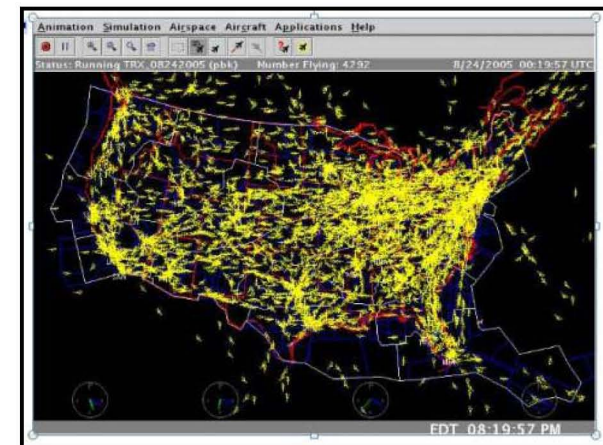
Benefits:

- Understanding the impact of degradations in **human performance** on **aircraft performance**.
- Identifying fleet-wide anomalies due to **mechanical and other related issues** that can impact safety, maintenance schedules, and operating cost.
- Development of advanced methods to **predict adverse events** due to **introduction** of new technologies in **NextGen**.

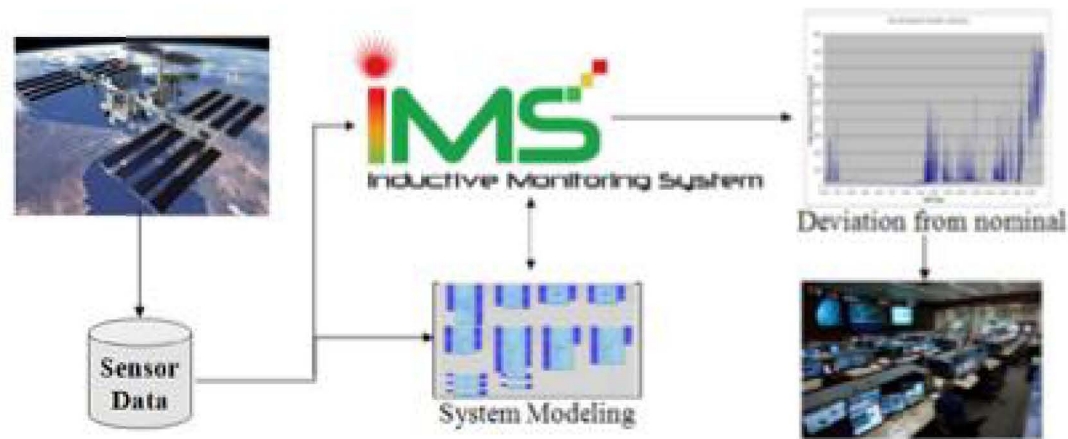


Sample Text Report

JUST PRIOR TO TOUCHDOWN,
LAX **TWR** TOLD US TO GO
AROUND BECAUSE OF THE
ACFT IN FRONT OF US. ...



Example Applications on ISS



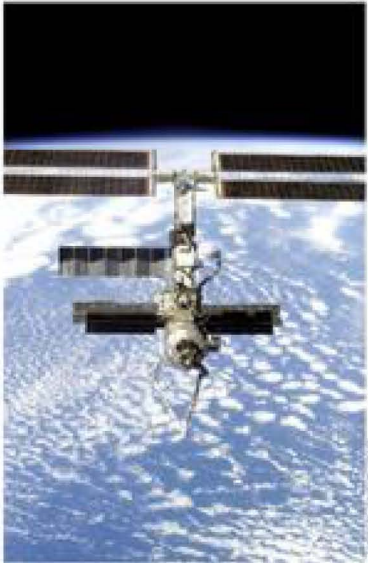
Automatically learns how the system typically behaves and tells you if it is behaving differently now

- Control Moment Gyros
- RGA
- ETCS
- ARJ
- Beta Gimbal Unit
- CDRA

ISS Early External Thermal Control System

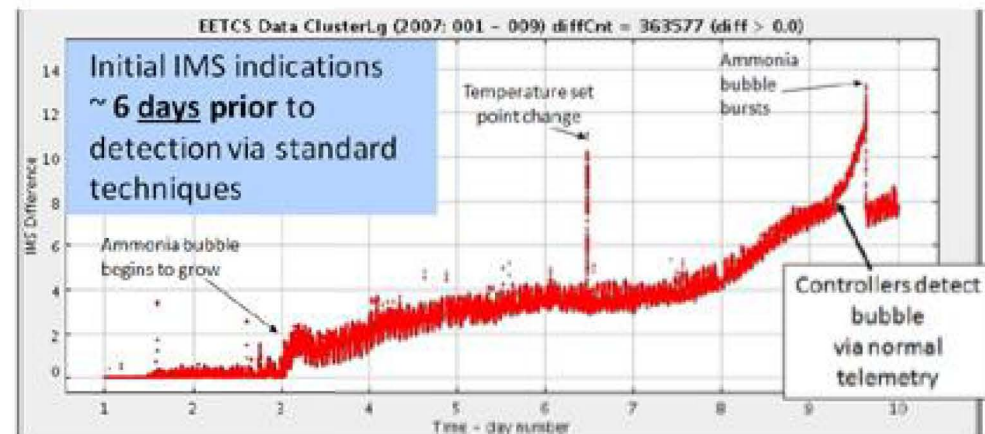


ISS Early External Thermal Control System (EETCS)



- EETCS used to dissipate heat on-board ISS
- Heat transferred to liquid ammonia cooling loops
- Ammonia circulated to external radiators to cool
- In early January 2007 EETCS developed an ammonia gas bubble
- Bubble noted by ISS controllers ~9 hours before it 'burst' and dissipated back into liquid

Results: ISS Early External Thermal Control System



- IMS trained on 185 days of data collected June - December 2006
- 23 parameters analyzed (pressures, temperatures, quantities, pump speeds)
- Z-score normalization, no external computations/derived parameters

Example Application on STS

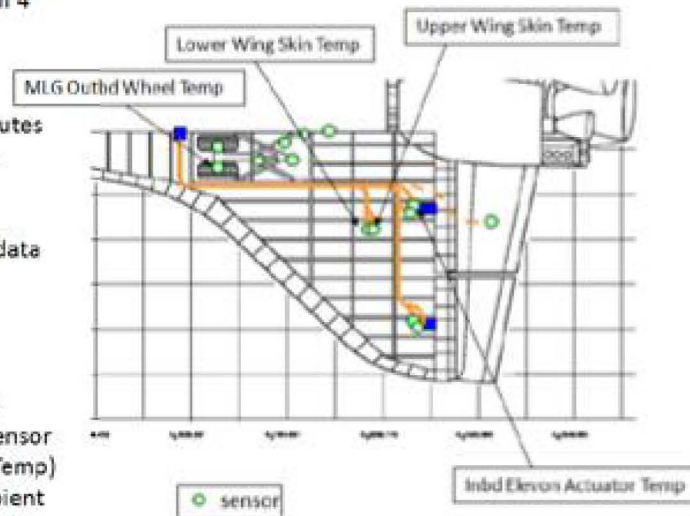


STS-107 Columbia Ascent IMS Analysis

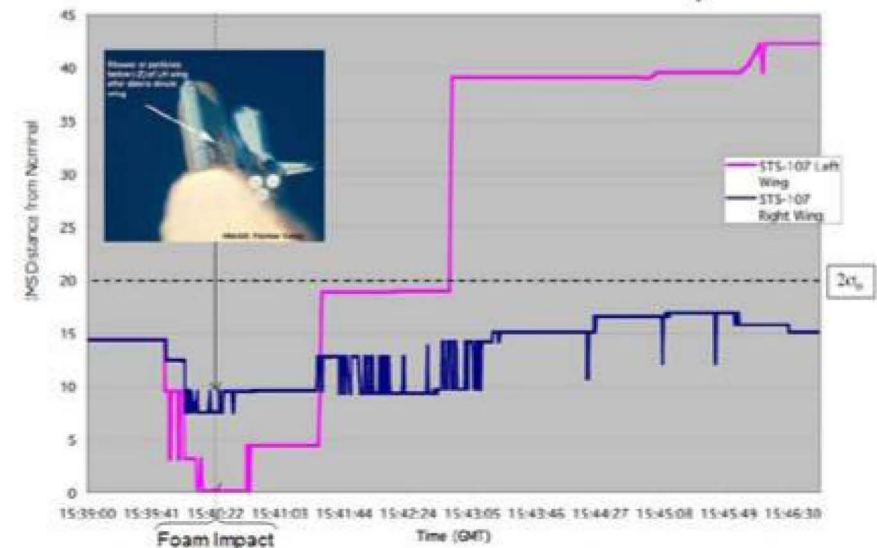
- Data vectors formed from 4 temperature sensors inside the wing
- Data covered first 8 minutes of each flight (Launch to Main Engine Cut Off)
- Trained on telemetered data from 10 previous Columbia flights

Normalization:

- Data expressed as value relative to a reference sensor (MLG Outboard Wheel Temp) to account for wide ambient temperature variations in training data



STS-107 Launch IMS Analysis



Example Application on STS



Space Shuttle Wing Leading Edge Impact Detection System (WLEIDS)

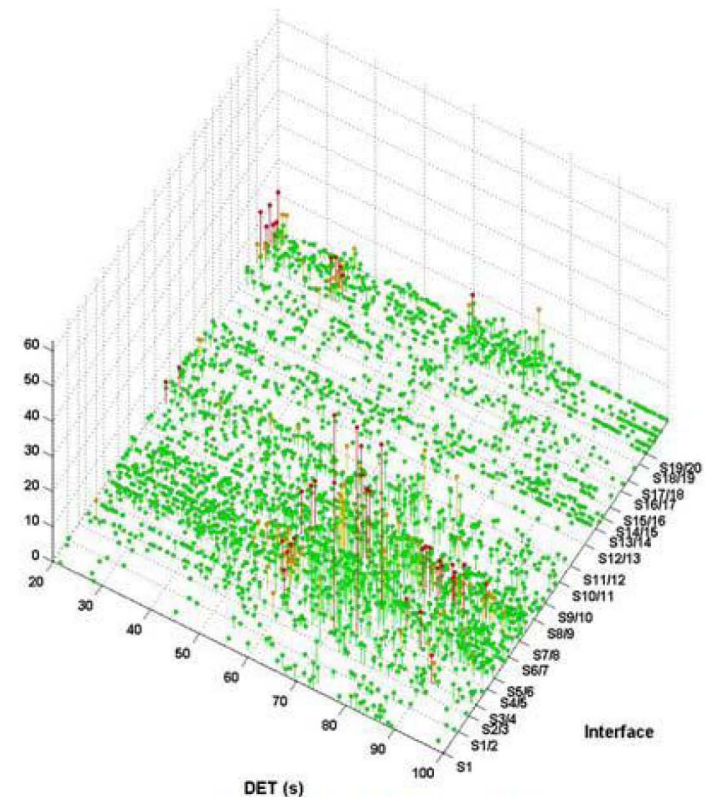


132 1-D accelerometers mounted on the wing spar behind RCC panels

20 KHz sensor data collected during ascent

Once on orbit, sensor data summary files transmitted to Mission Control for analysis

Orca/IMS vectors constructed from 8 sensor values, including a target sensor and surrounding sensors that might pick up radiating impact energy



Points of Interest
Detected by Orca/IMS

Technical Challenge 3

Automation Design Tools

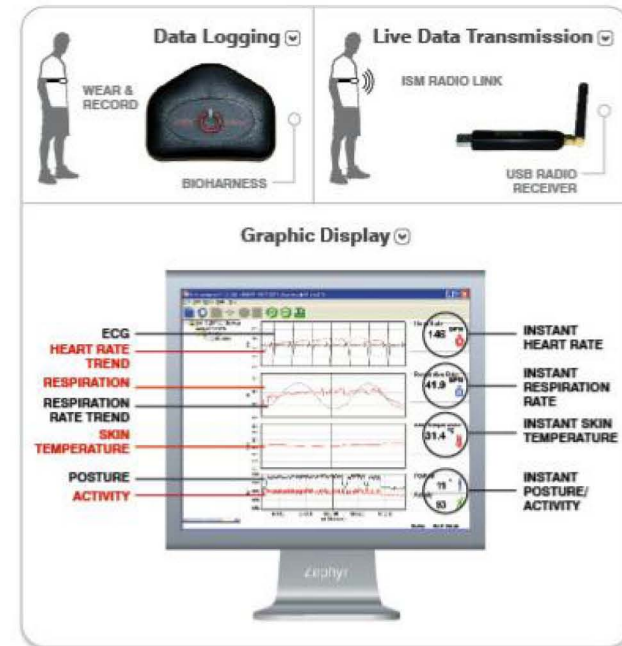


Advancing Safety by Understanding Human Performance

Develop analysis tools that incorporate known **limitations** of **human performance** and enable design of robust **human-automation systems** to increase **safety** and **reduce validation costs** in NextGen (FY 20).

Benefits:

- Methods and tools appropriate for **designers, trainers, and operators.**
- Enable the **prediction of human performance** to **identify, evaluate, and resolve safety issues** due to Human – Automation interaction.

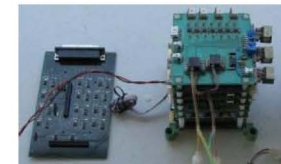


Technical Challenge 4

Prognostic Algorithms for Safety Assurance



Prognostic Algorithm Design for Safety Assurance

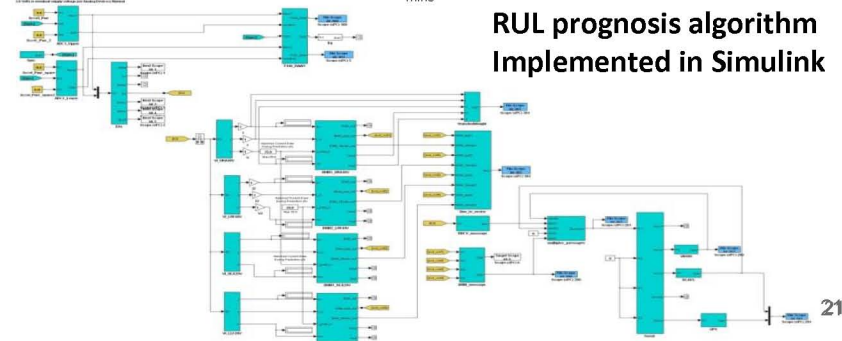
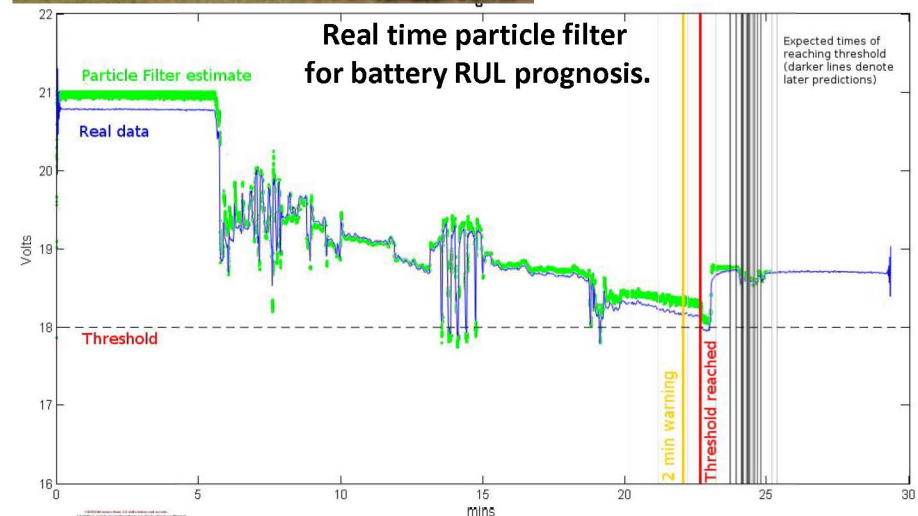


BHM hardware & Real time CPU

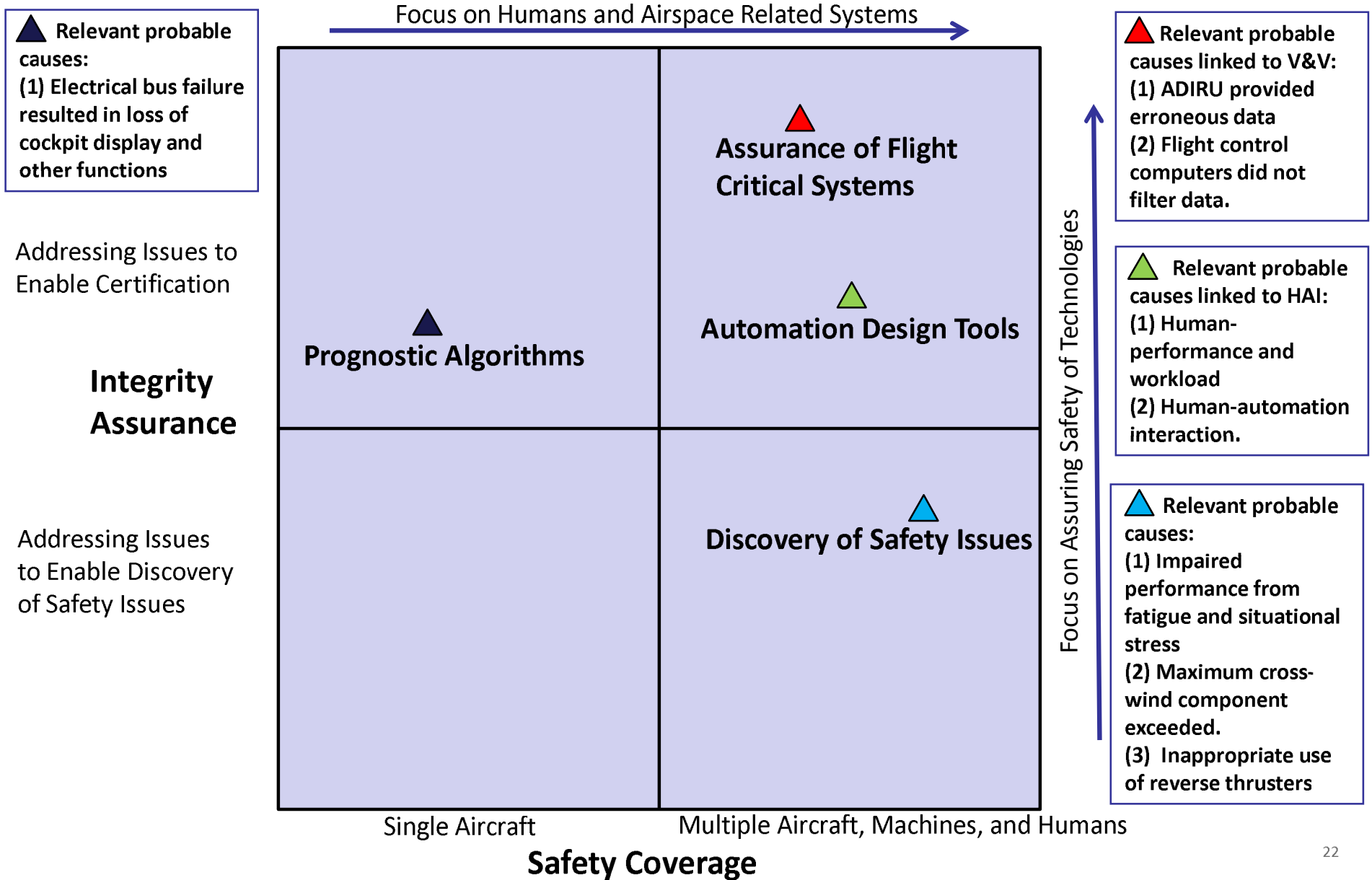
Development of a new class of **verifiable prognostic algorithms** to help **remove obstacles** to the **certification** of prognostic algorithms (FY25).

Benefits: .

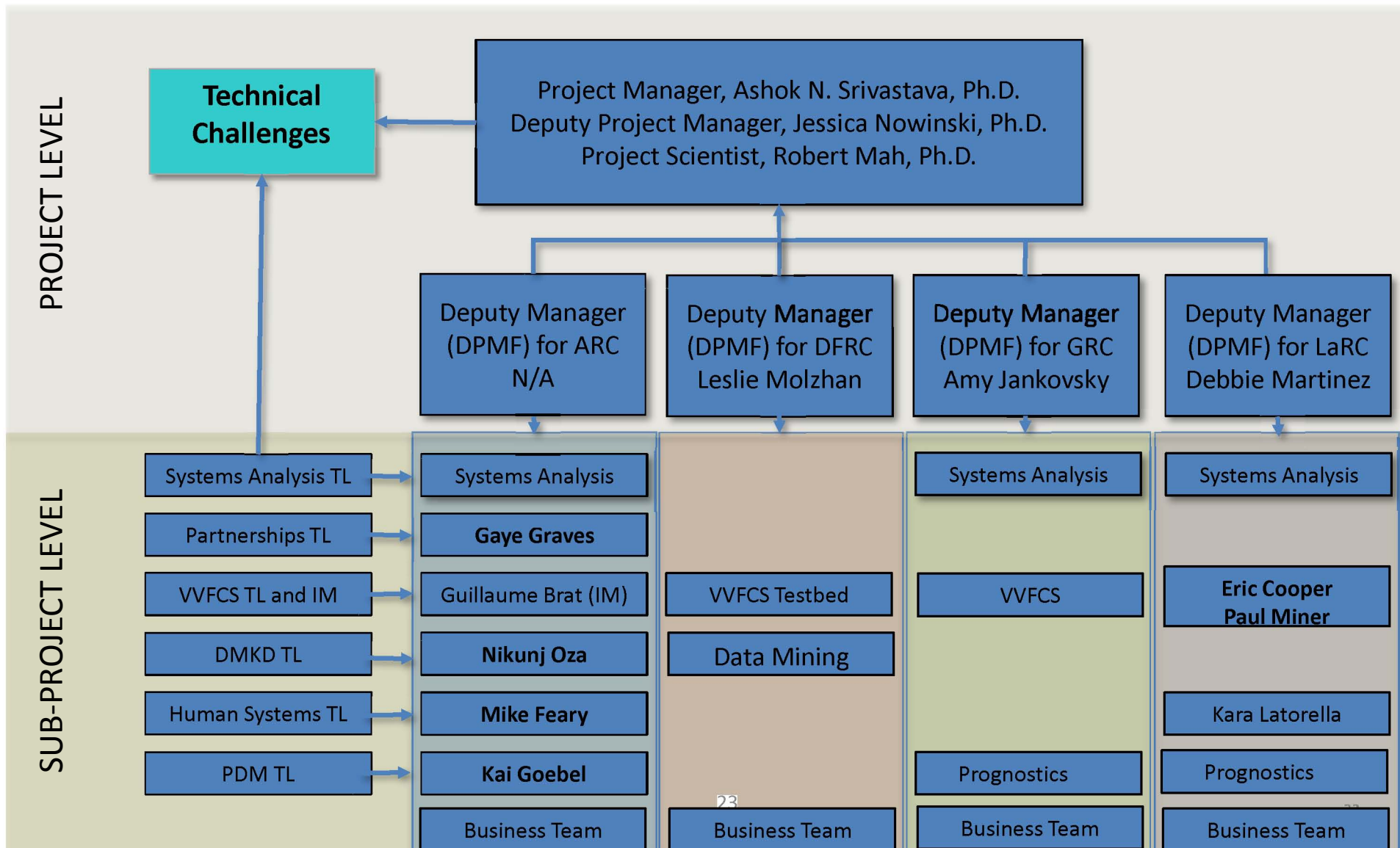
- **New class** of verifiable systems health management algorithms and methods.
- **Lowered barrier** to deployment of systems health management algorithms.



SSAT Technical Challenges Cover a Broad Range of Safety and Assurance Technologies



SSAT Project Organizational Structure



SSAT Partnership Strategy



SSAT develops partners based on a strategic need (as assessed by the Project Management Team) in the following areas:




- Access to **data** not readily available to NASA that is directly related to a Tech Challenge
- **Experimental platforms** and unique expertise directly related to a Tech Challenge
- Unique test, integration, and **infusion opportunities**

We are frequently approached for potential partnerships from domestic and international government agencies, academic institutions, air carriers, and major industry players.

	<p>Validation of data mining algorithms for discovering precursors to aviation safety incidents.</p>
	<p>Research Test and Integration Collaborations</p> <ul style="list-style-type: none"> • Partial list of partners supporting collaborative research • Prognostic algorithms for EMA; integrated research on Engine Fault Detection and Diagnosis • V&V and Software Health Management • Pilot fatigue (SOFIA, Air Force) • Support research in Airspace Concepts






Overview- SSAT Partnerships (II)



	<p>Assessment of current Systems Health Management capabilities and emerging technologies for V&V, Data Mining, Human Automation and Interaction Tools, and Prognostics/Decision Making; development of an analytical framework for evaluation and benchmarking of these technologies; and collaboration in health management data and algorithms.</p>
<p>VSST / AEST</p>	<ul style="list-style-type: none"> • System architecture to enable resilient flight deck automation technologies based on the output of the Vehicle Level Reasoning System. • Vehicle level detection and diagnosis of sensor and actuator faults; application of virtual sensor technology; system architecture to enable resilient adaptive control based on the output of the Vehicle Level Reasoning System.
	<ul style="list-style-type: none"> • Vehicle-level architecture and reasoner • Ground to flight architectures and testbeds • IVHM-enabled CBM • Data Mining 























Overview - SSAT Partnerships (III)



 	<p>Validation of methods to discover precursors to aviation safety incidents and the impact of pilot fatigue.</p>
 	<p>Cooperative research and technology development (R&TD) activities in the areas of V&V, data mining, and human automation and interaction tool technologies and systems.</p>
	<p>Prognostics of composites. (SAA)</p>
<p>Airspace Systems Program</p>	<p>Co-funding CMU NRA for demonstrating compositional verification on separation assurance software</p>
<p>Networking and Information Technology Research and Development Source (NITRD)</p>	<p>Participation/representation for three NITRD Program Coordination Areas: High Confidence Software and Systems; Software Design & Productivity Human Computer Interaction & Information Management</p>
<p>Joint Safety Analysis Team (JSAT)</p>	<p>Year long collaboration and membership regarding the use of data mining to discover precursors to safety incidents</p>

SSAT Research Partners



<p><u>Assurance of Flight Critical Systems</u> (including Software Health Management)</p>	          
<p><u>Discovery of Safety Issues</u></p>	  
<p><u>Automation Design Tools</u></p>	 
<p><u>Prognostic Algorithm Design for Safety Assurance</u></p>	     

Progress Metrics for SSAT Research

A Model-Based Approach



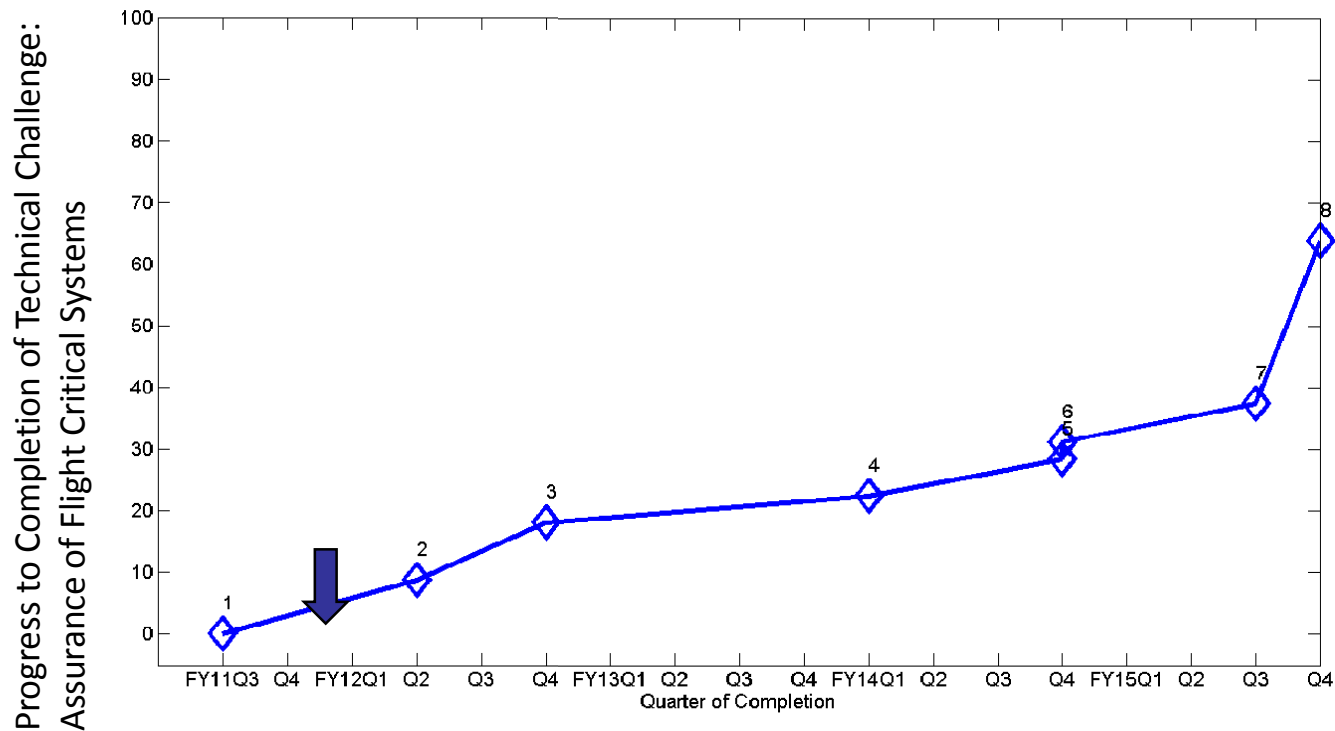
- SSAT used a **model-based approach** to assess **the impact of our research and progress** toward meeting our TC. Uncertainty of progress metric increases with time.
- The assumptions have been **validated** with the Technical Leads and DPMFs.
- These metrics give only **one assessment** of the progress towards solution of the challenge. There are other ways to demonstrate the progress and impact of our research.
- Models incorporate **an assessment of probability of technical infusion**, thus helping to address progress towards completion of TC.
- About the Models
 - Model parameters **can be changed** based on new information and can be used to perform **'what-if analysis'**, such as, 'what if our research produces a 20% improvement in accuracy instead of a 10% improvement?'
 - The models include factors that are **'hard-benefits'** such as improvements in accuracy, speed, etc., and **'soft-benefits'** such as 'improvement in query technologies'.
 - The models include a parameter that assess the **likelihood of technology transition** into a real-world implementation (not just transition from NASA to industry).
 - The models are **tied to overarching safety goals** with specific Aviation Safety **incidents and accidents cited** using an approach similar to that used in the IT industry.
- SSAT will update these models routinely to maintain relevance to Tech Challenges and changing research results and needs.

All models are wrong, but some are useful- G. E. P. Box



Progress to Completion of Technical Challenge 1

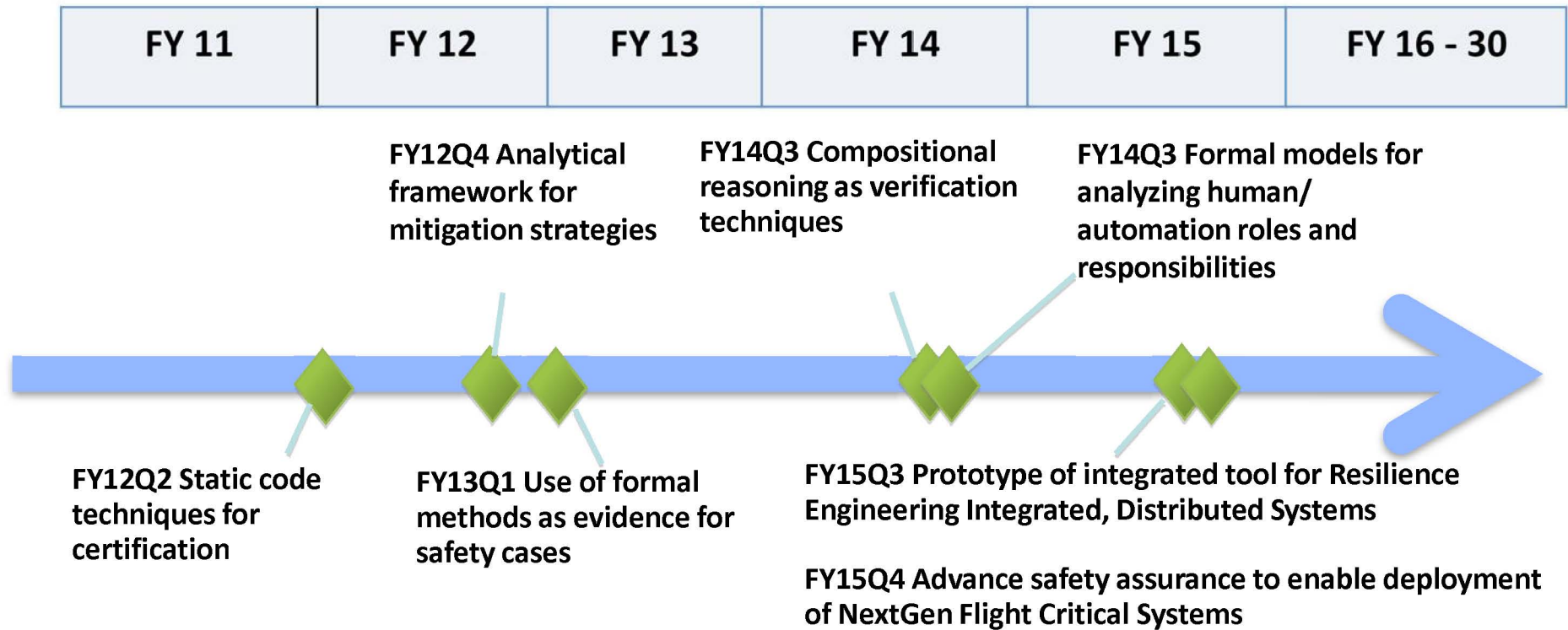
Assurance of Flight Critical Systems



- 1 Baseline
- 2 Static code techniques for certification
- 3 Analytical framework for mitigation strategies
- 4 Use of formal methods as evidence for safety cases
- 5 Compositional reasoning as verification techniques
- 6 Formal models for analyzing human/automation roles and responsibilities
- 7 Prototype of integrated tool for resilience engineering for integrated distributed systems
- 8 Advance safety assurance to enable deployment of NextGen flight critical systems

Measuring Progress

Assurance of Flight Critical Systems



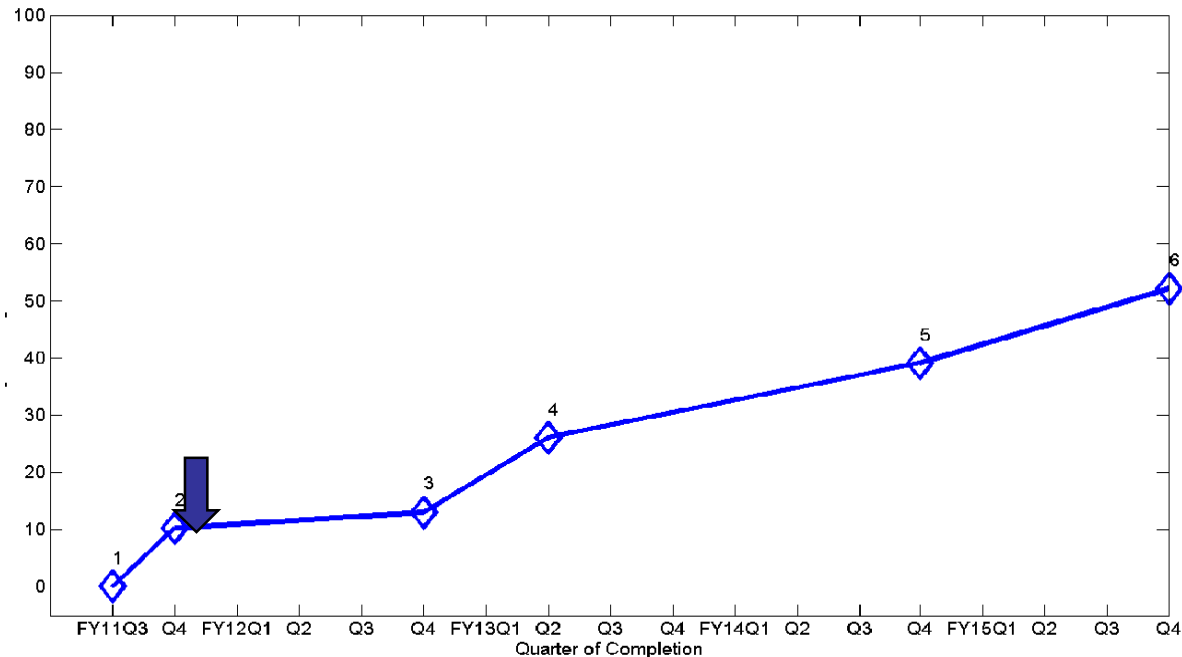
What are the intermediate and final exams to check for success?

- Demonstration of a 0% false positive rate by combining static analysis and model checking
- Development of validated communication topologies
- Unified approach to autonomy and authority

Progress to Completion of Technical Challenge Discovery of Safety Issues



Progress to Completion of Technical Challenge:
Discovery of Safety Issues



- 1 Baseline
- 2 Scalable algorithm for anomaly detection on heterogeneous data
- 3 Scalable algorithm for prediction of prescribed adverse events in discrete and continuous data
- 4 Vehicle Level Reasoning
- 5 Identification of precursors in flight and text data
- 6 Automated discovery of precursors to safety incidents

Measuring Progress Discovery of Safety Issues

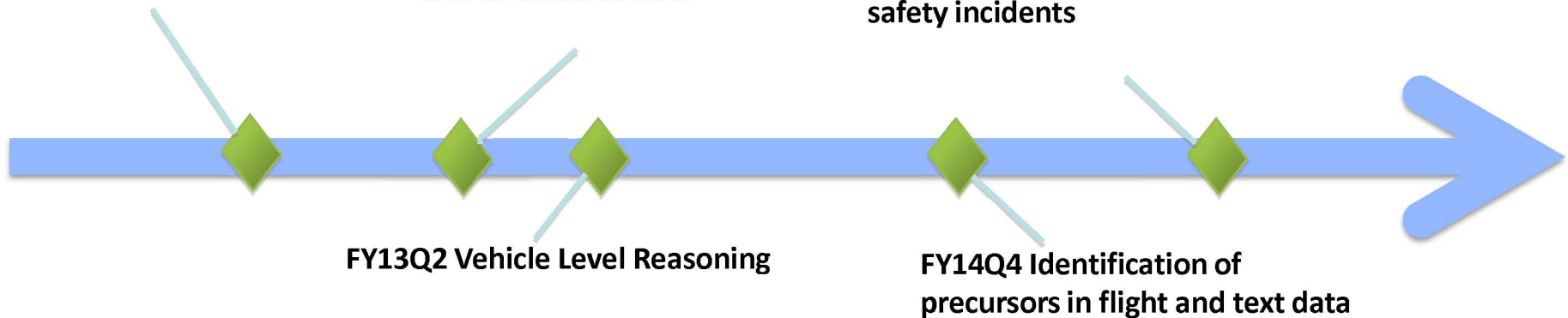


FY 11	FY 12	FY 13	FY 14	FY 15	FY 16 - 30
-------	-------	-------	-------	-------	------------

FY11Q4 Scalable algorithm for anomaly detection on heterogeneous data

FY12Q4 Scalable algorithm for prediction of prescribed adverse events in discrete and continuous data

FY15Q4 Automated discovery of precursors to safety incidents

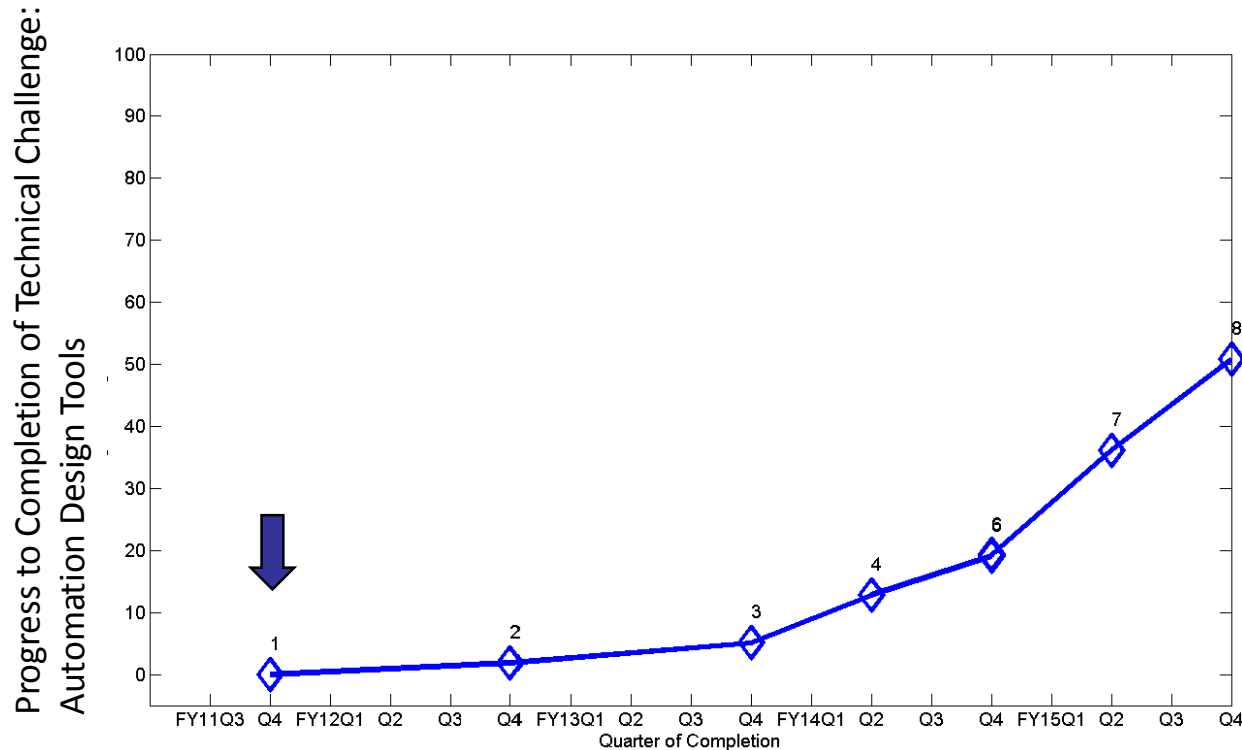


What are the intermediate and final exams to check for success?

- Development of methods to analyze 10 TB of heterogeneous data
- Development of methods to identify crew performance degradation
- Development of predictive methods for heterogeneous data sets.

Progress to Completion of Technical Challenge

Automation Design Tools



- 1 Baseline
- 2 Methods for determining functional state in operations
Develop technologies to provide early detection and mitigation of flight crew performance issues, using unobtrusive behavior monitoring.
- 3
- 4 Tools for evaluation of human - automation procedural complexity
- 5 Predictive Human Performance Design Tools
Develop toolbox and guidelines for incorporating multimodal information management strategy
- 6
- 7 Identification of novel Human-Automation Interaction Failures
- 8 Human Automation Design Tools

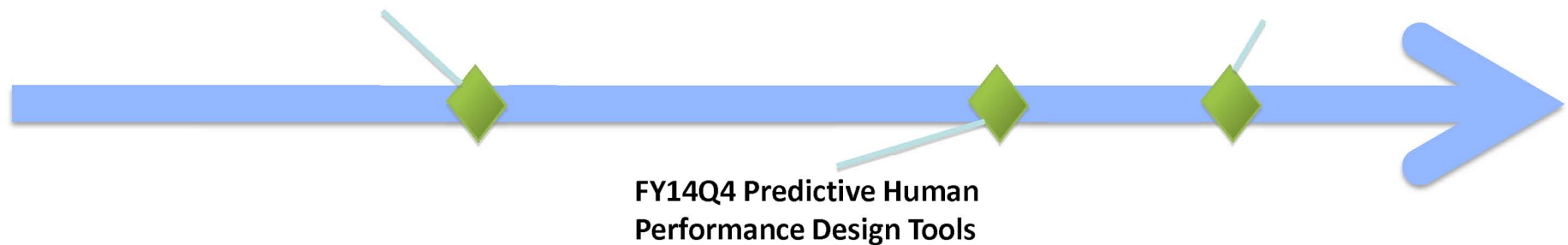
Measuring Progress Automation Design Tools



FY 11	FY 12	FY 13	FY 14	FY 15	FY 16 - 30
-------	-------	-------	-------	-------	------------

FY12Q4 Methods for determining human functional state in operations

FY15Q4 Identification of novel Human – Automation Interaction failures, Human Automation Design Tools

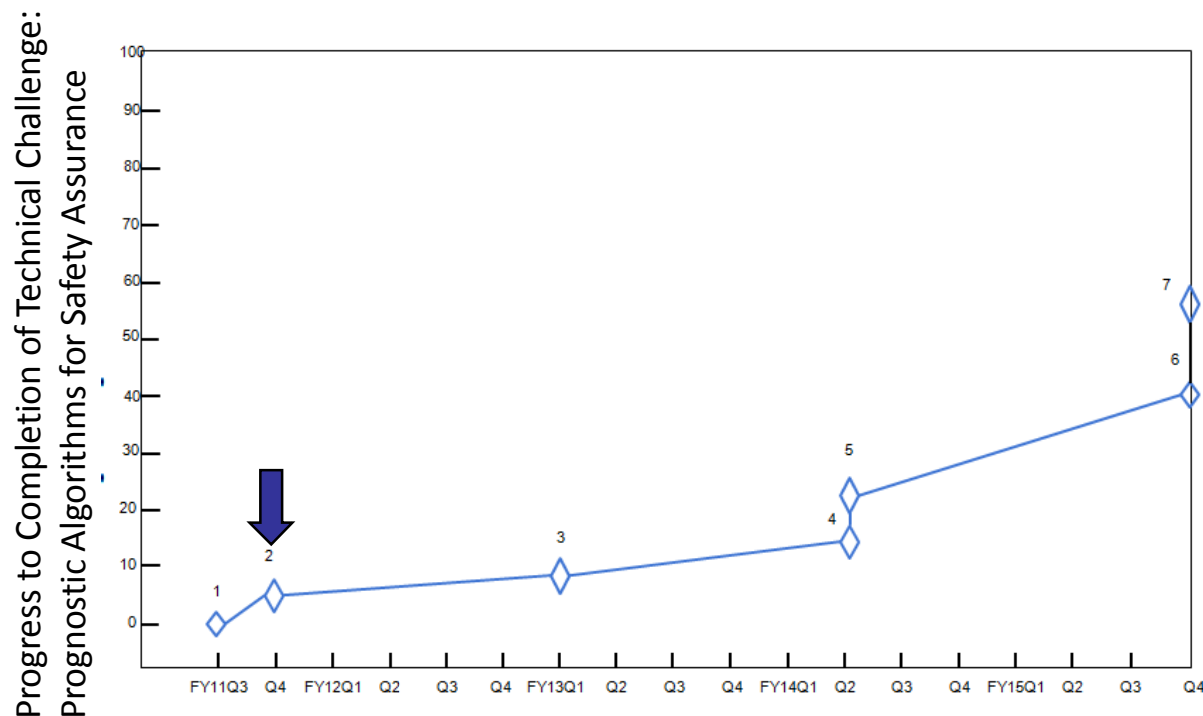


What are the intermediate and final exams to check for success?

- Proof-of-concept tools demonstrating the ability to support the design validation and verification process; Framework reviewed by subject matter experts.
- Proof-of-concept Matlab based visualization tool suite for monotonic analog signals arising from sensor and performance based aircraft operations or faults.

Progress to Completion of Technical Challenge

Prognostic Algorithms for Safety Assurance



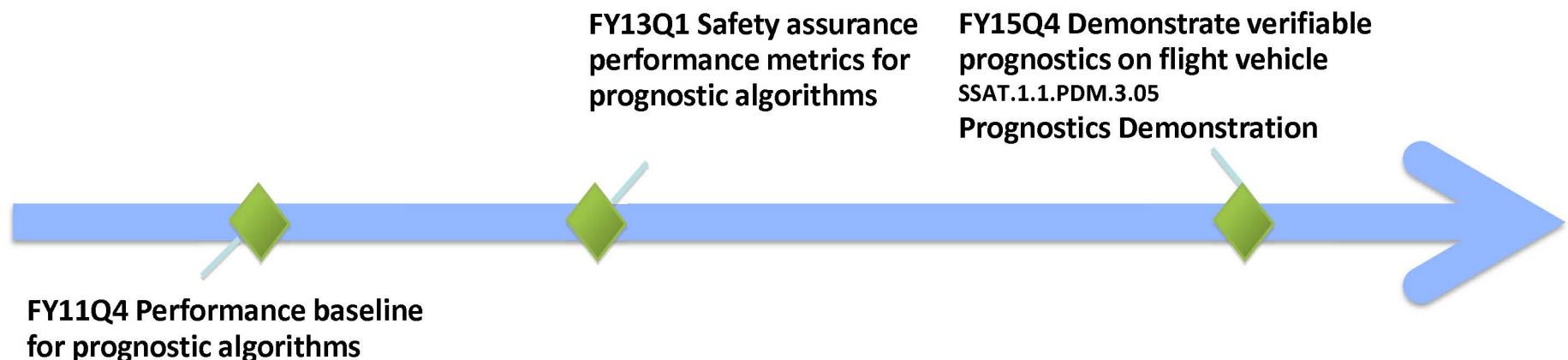
- 1 Baseline
- 2 Performance baseline for prognostic algorithms
- 3 Safety Assurance performance metrics for prognostic algorithms
- 4 Demonstrate mission extension
- 5 Integrated Decision Making
- 6 Demonstrate avoidance of mission abort
- 7 Demonstrate verifiable prognostics on flight vehicle

Measuring Progress

Prognostics Algorithms for Safety Assurance



FY 11	FY 12	FY 13	FY 14	FY 15	FY 16 - 30
-------	-------	-------	-------	-------	------------



What are the intermediate and final exams to check for success?

- Demonstrate the prognostics algorithm meets the verifiability metric previously identified, and demonstrate using a flight vehicle that the previously identified performance metric is met.
- Provide metrics, methods, and tools to VSST for integration.
- Investigate diagnostic and/or prognostic algorithm with respect to: (1) verifiability; (2) ability to distill varying degrees of knowledge of underlying physics; (3) ability to process varying degrees of knowledge about uncertainty

SSAT Project Technical Challenges

Annual Performance Goal (APG)

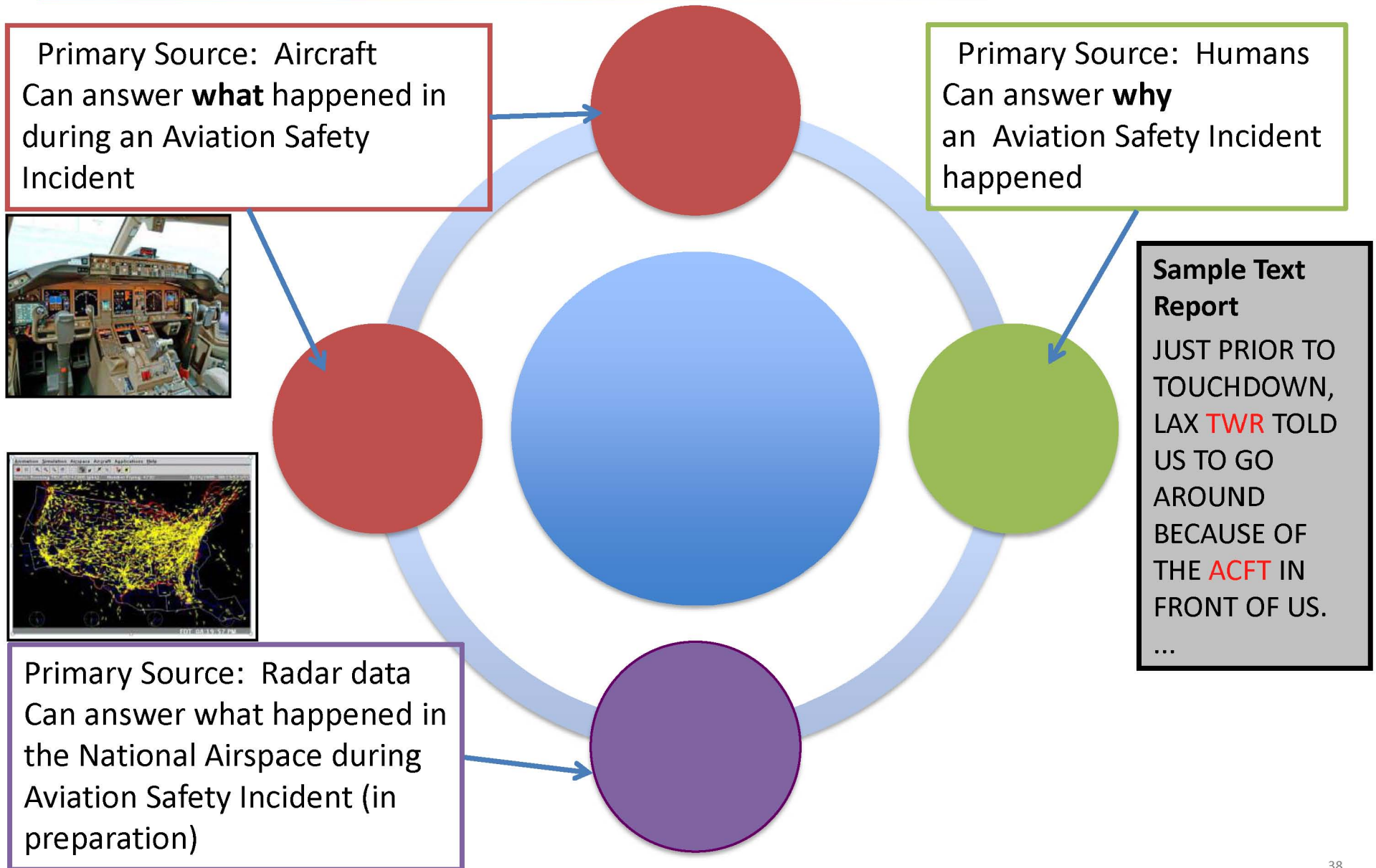


EXAMPLE (FY11/FY12)

Data Mining - Scalable anomaly detection on heterogeneous data

- Description: Development of a **scalable algorithm** for anomaly detection on data consisting of discrete and continuous sequences as well as text reports that have been matched up (i.e., are from the same flight).
- Metric/Exit Criteria: Algorithm that identifies at least **three anomalies** (in real flight data) validated by an expert to be statistical anomalies. Run time should be nominally **no more than 50% greater** than the run time for the fastest algorithm that runs on only discrete and continuous sequences.

Mining Heterogeneous Data is the Key



Knowledge Dissemination



Conferences	141
Journal Articles	44
NASA Technical Manuscripts	4
Book Chapters & Contractor Reports	16
Books	2
DASHlink Downloads (Papers, Code, and Data)	Approximately 3000 downloads per month

8 Awards at Major International Conferences:

- IEEE International Conference on Data Mining
- IEEE International Conference on Systems, Man, and Cybernetics
- Prognostics and Health Management Society
- Surface Mount Technology Association
- Autotestcon

[Login](#) | [Register](#)

[HOME](#) [RESEARCH AREAS](#) [PROJECTS](#) [RESOURCES](#) [MEMBERS](#)

A web-based collaboration tool for those interested in data mining and systems health

LEARN MORE

Research Areas
 Learn about our research fields, goals and their associated projects.

Projects
 See what others in the community are working on. Join or start your own.

Resources
 Available data sets, algorithms, and publications FREE to download

Impact of the SSAT Project



SSAT and IVHM influenced the design of the Central Maintenance Computer of the 787, Embraer, and other major jets.

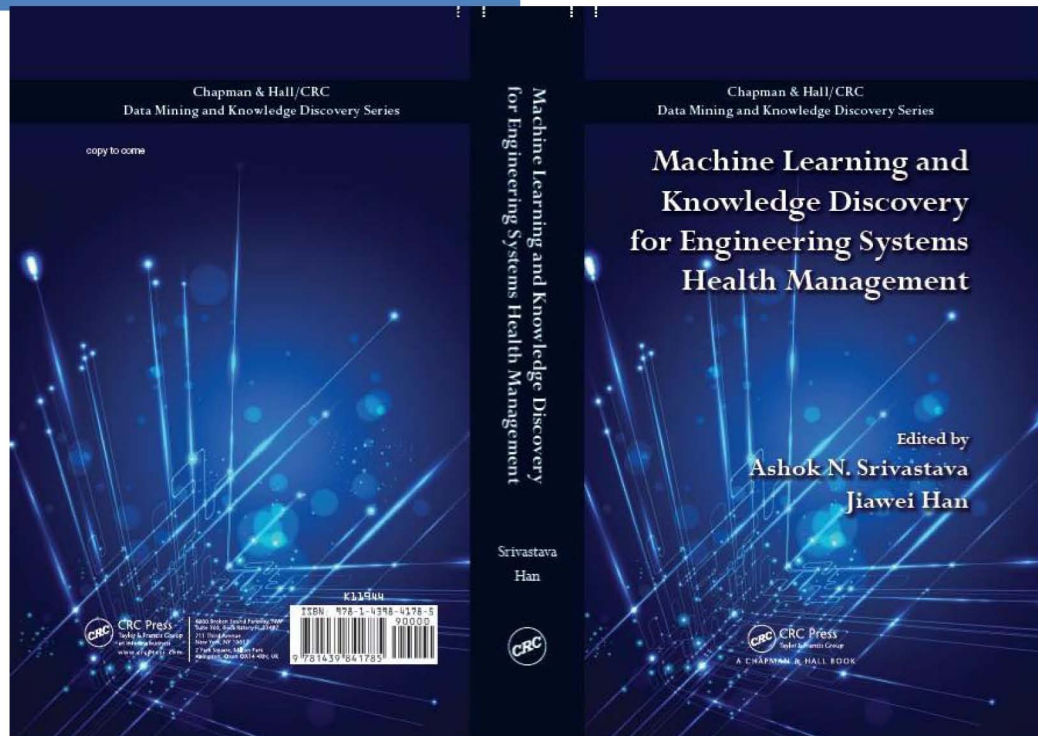
Transfer of ADEPT Software to Gulfstream to help design and analyze new concepts for controlling system functions.

Fatigue Risk Management Studies at EasyJet and Onera are underway with both NASA Technical Reports published.

Southwest Airlines utilizing data mining to improve safety of current operations.

142 Conference Papers
48 Journal Papers
10 NASA Technical Manuscripts
16 Book Chapters + Reports
4 Invention Disclosures
2 Books

- Top 10 Data Mining Case Study at IEEE ICDM Conference
- 8 Best Paper Awards





THANK YOU