NASA SBIR 2019 Phase I Solicitation

S5.05 Fault Management Technologies

Lead Center: JPL

Participating Center(s): ARC, MSFC

Technology Area: TA4 Robotics, Telerobotics and Autonomous Systems

Development, Design, and Implementation of Fault Management Technologies

NASA's science program has well over 100 spacecraft in operation, formulation, or development, generating science data accessible to researchers everywhere. As science missions are given increasingly complex goals, often on compressed timetables, and have more pressure to reduce operations costs, system autonomy must increase in response. Fault Management (FM) is one of the key components of system autonomy.

FM consists of operational mitigations of spacecraft failures and is implemented with spacecraft hardware and on-board autonomous software that controls hardware, software, and information redundancy, in concert with ground-based software and operations procedures. Despite a wealth of lessons learned from past missions, spacecraft failures are still not uncommon, and reuse of FM approaches is very limited, illustrating that advancements are needed in FM Design Tools, FM Visualization Tools, FM Operations Approaches, FM Verification and Validation Tools, and FM

Design Architectures.

The specific objectives of this subtopic are to improve FM technologies and approaches, as follows:

- Improve predictability of FM system complexity and estimates of development and operations costs
- Enable cost-effective FM design architectures and operations
- Determine completeness and appropriateness of FM designs and implementations
- Decrease the labor and time required to develop and test FM models and algorithms
- Improve visualization of the full FM design across hardware, software, and operations procedures
- Determine extent of testing required to verify FM, particularly where model-based, and estimate the potential risk resulting from incomplete coverage
- Increase data integrity between multi-discipline tools
- Standardize metrics and calculations across FM, SE, S&MA and operations disciplines
- Increase reliability of FM systems

Specific technology advancements in the areas listed below are needed to improve the capability of fielded FM systems. Guidance for development can be found in the NASA FM Handbook:

- *FM Design Tools* - System modeling and analysis significantly contributes to the quality of FM design, and

may prove decisive in trades of new vs. traditional FM approaches. However, the difficulty in translating system design information into system models often impacts modeling and analysis accuracy. Examples of enabling techniques and tools are automated modeling systems, spacecraft modeling libraries, expedited algorithm development, sensor placement analyses, and system model tool integration.

- *FM Visualization Tools* - FM systems incorporate hardware, software, and operations mechanisms. The ability to visualize the full FM system and the contribution of each component to protecting mission functions and assets is critical to assessing the completeness and appropriateness of the FM design to the mission attributes (mission type, risk posture, operations concept, etc.). Fault trees and state transition diagrams are examples of visualization tools that contribute to visualization of the full FM design.
- *FM Operations Approaches* - Typical FM processes attempt to preserve the asset in the event of detected anomalies by safing the vehicle and relying on mission operations to determine how to proceed. However, many new mission concepts require greater autonomy – for example, riding out failures or autonomously restarting system behavior in order to complete science objectives that require timely operations. Future spacecraft must be able to make decisions about how to recover from failures or degradations and continue the mission. FM designs must enable flexible operations that can integrate on-board decision-making with input from mission operations.
- *FM Verification and Validation Tools* - Along with difficulties in system engineering, the challenge of V&V'ing new FM technologies has been a significant barrier to infusion in flight projects. As complexity of spacecraft and systems increases, the testing required to verify and validate FM implementations can become prohibitively resource intensive without new approaches. Automated test case development, false positive/false negative test tools, model verification and validation tools, and test coverage risk assessments are examples of contributing technologies.
- *FM Design Architectures* - FM capabilities may be implemented through numerous system, hardware, and software architecture solutions. The FM architecture trade space includes options such as embedding within the flight control software or deployment as independent onboard software; on-board versus ground-based capabilities; centralized or distributed FM functions; sensor suite implications; integration of multiple FM techniques; innovative software FM architectures implemented on flight processors or on Field Programmable Gate Arrays (FPGAs); and execution in real-time or off-line analysis post-operations. Alternative architecture choices such as model-based approaches could help control FM system complexity and cost and could offer solutions to transparency, verifiability, and completeness challenges.
- *Multi-discipline FM Interoperation* - FM designers, Systems Engineering, Safety and Mission Assurance, and Operations all perform analyses and assessments of system reliability, failure modes and effects, sensor coverage, failure probabilities, anomaly detection and response, contingency operations, etc. These analyses are highly sensitive to inconsistencies and misinterpretations of multi-discipline data, resulting in higher costs to resolve disconnects in data and analyses, or even reducing mission success due to failure modes that were overlooked. Solutions that address data integrity, identification of metrics, and standardization of data products, techniques and analyses will reduce cost and failures.

Expected outcomes are better estimation and control of FM complexity and development costs, improved FM designs, and accelerated advancement of FM tools and techniques.

FM technologies are applicable to all Science Mission Directorate (SMD) missions, with particular emphasis on medium to large missions as these have much lower tolerance for risk, representing substantial potential benefit. A few examples are provided below, although these may be generalized to a broad class of missions:

- *Europa Exploration (Clipper and Lander)* - Provide on-board capability to detect and correct radiation-induced execution errors. Provide reliable reasoning capability to restart observations after interruptions without requiring ground in-the-loop. Provide MBSE tools to model and analyze FM capabilities in support of design trades, V&V of FM capabilities, and coordinated development with flight software.
- *Mars Exploration (Rovers and Sample Return)* - Provide on-board capability for systems checkout, enabling mobility after environmentally-induced anomalies (e.g., unexpected terrain interaction). Improve reliability of complex activities (e.g., drilling and sample capture, capsule pickup and remote launch).
- *Search for Extrasolar Planets (Observation)* - Provide sufficient system reliability through on-board detection, reasoning, and response to enable long-period, stable observations. Provide on-board or on-ground analysis capabilities to predict system response and optimize observation schedule. Enable reliable operations while out of direct contact (e.g., deliberately occluded from Earth to reduce photon, thermal, and radio frequency background).

It is intended that proposed efforts conduct an initial proof of concept, after which successful efforts would be considered for follow-on funding by SMD missions as risk-reduction and infusion activities. Research should be conducted to demonstrate technical feasibility and NASA relevance during Phase I and show a path toward a Phase II prototype demonstration.

Accordingly, the Final Report should thoroughly document the innovation, its status at the end of the effort, and as much objective evaluation of its strengths and weaknesses as is practical. The report should include a description of the approach, foundational concepts and operating theory, mathematical basis, and requirements for application. Results should include strengths and weaknesses found, measured performance in tests where possible.

Additional deliverables may significantly clarify the value and feasibility of the innovation. These deliverables should be planned to demonstrate retirement of development risk, increasing maturity, and targeted applications of particular interest. While the wide range of innovations precludes a specific list, some possible deliverables are listed below:

- For innovations that are algorithmic in nature, this could include development code or prototype applications, demonstrations of capability, and results of algorithm stress-testing.
- For innovations that are procedural in nature, this may include sample artifacts such as workflows, model prototypes and schema, functional diagrams, example or tutorial applications.
- Where a suitable test problem can be found, documentation of the test problem and a report on test results, illustrating the nature of the innovation in a quantifiable and reproducible way. Test reports should discuss maturation of the technology, implementation difficulties encountered and overcome, results and interpretation.

The expected Technology Readiness Level (TRL) range at completion of the project is 3-4.

References:

- NASA Fault Management Handbook (https://www.nasa.gov/pdf/636372main_NASA-HDBK-1002_Draft.pdf)
- Talks presented at the 2012 FM Workshop:
    - https://www.nasa.gov/offices/oce/documents/2012_fm_workshop.html
    - https://www.nasa.gov/pdf/637595main_day_1-brian_muirhead.pdf
- NASA Technical Memorandum "Introduction to System Health Engineering and Management for Aerospace (ISHEM)" (https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20060003929.pdf)
- Johnson, S. (ed), System Health Management with Aerospace Applications, Wiley, 2011 (https://www.wiley.com/en-us/System+Health+Management%3A+with+Aerospace+Applications-p-9781119998730)