



NASA SBIR 2016 Phase I Solicitation

S5.05 Fault Management Technologies

Lead Center: ARC

Participating Center(s): JPL, MSFC

As science missions are given increasingly complex goals and have more pressure to reduce operations costs, system autonomy increases. Fault Management (FM) is one of the key components of system autonomy. FM consists of the operational mitigations of spacecraft failures. It is implemented with spacecraft hardware, on-board autonomous software that controls hardware, software, information redundancy, and ground-based software and operations procedures.

Many recent Science Mission Directorate (SMD) missions have encountered major cost overruns and schedule slips during test and verification of FM functions. These overruns are due to a lack of understanding of FM functions early in the mission definition cycles and to FM architectures that do not provide attributes of transparency, verifiability, fault isolation capability, or fault coverage. The NASA FM Handbook is under development to improve the FM design, development, verification and validation and operations processes. FM approaches, architectures, and tools are needed to improve early understanding of needed FM capabilities by project managers and FM engineers and to improve the efficiency of implementing and testing FM.

Specific objectives are to:

- Improve the ability to predict FM system complexity and estimate 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, completeness of verification planned, and residual 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.

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

The approach of this subtopic is to seek the right balance between sufficient reliability and cost appropriate to the mission type and risk posture. Successful technology development efforts under this subtopic would be considered for follow-on funding by, and infusion into, SMD missions. Research should be conducted to demonstrate technical feasibility and NASA relevance during Phase I and show a path toward a Phase II prototype demonstration.

Offerors should demonstrate awareness of the state-of-the-art of their proposed technology, and should leverage

existing commercial capabilities and research efforts where appropriate.

Specific technology in the forms listed below is needed to increase delivery of high quality FM systems. These approaches, architectures and tools must be consistent with and enable the NASA FM Handbook concepts and processes:

- *FM Design Tools* - System modeling and analyses significantly contributes to the quality of FM design; however, the time it takes to translate system design information into system models often decreases the value of the modeling and analysis results. Examples of enabling techniques and tools are modeling automation, 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 mechanism 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 could contribute to visualization of the full FM design.
- *FM Verification and Validation Tools* - As complexity of spacecraft and systems increases, the extensiveness of testing required to verify and validate FM implementations can be resource intensive. 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 embedded in the flight control software or 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 perform analyses and assessments of reliabilities, failure modes and effects, sensor coverage, failure probabilities, anomaly detection and response, contingency operations, etc. The relationships between multi-discipline data and analyses are inconsistent and misinterpreted. Resources are expended either in effort to resolve disconnects in data and analyses or worse, reduced 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.