NASA SBIR 2020 Phase I Solicitation

S5.05 Fault Management Technologies

Lead Center: JPL

Participating Center(s): ARC, MSFC

Technology Area: TA4 Robotics, Telerobotics and Autonomous Systems

Scope Title Development, Design, and Implementation of Fault Management Technologies**Scope Description**NASA's science program has well over 100 spacecraft in operation, formulation, or development, generating science data accessible to researchers everywhere. As science missions have 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 a key component of system autonomy, serving to detect, interpret, and mitigate failures that threaten mission success. Robust FM must address the full range of hardware failures, but also must consider failure of sensors or the flow of sensor data, harmful or unexpected system interaction with the environment, and problems due to faults in software or incorrect control inputs -- including failure of autonomy components themselves.Despite a wealth of lessons learned from past missions, spacecraft failures are still not uncommon and reuse of FM approaches is very limited, illustrating deficiencies our approach to handling faults in all phases of the flight project lifecycle. While this subtopic addresses particular interest in on-board Fault Management capabilities (viz. on-board sensing approaches, computing, algorithms, and models to assess and maintain spacecraft health), the goal isto provide a *system capability*, and thus off-board components such as modeling techniques and tools, development environments, testbeds, and verification and validation (V&V) technologies are also relevant. Specific algorithms and sensor technologies are in scope provided their impact is not limited to a particular subsystem, mission goal, or failure mechanism.Innovations in Fault Management can be grouped into the categories below.

- Fault Management 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, algorithm prototyping and test environments, sensor placement analyses, and system modeling that supports multiple autonomy functions including FM. System design should enable multi-disciplinary assessment of FM approaches, addressing performance metrics, standardization of data products and models, and analyses to reduce design costs and design escapes.
- Fault Management Visualization Tools: FM systems have impacts on hardware, software, and operations. The ability to visualize the full FM system behavior and the contribution of each component to protecting mission functions and assets is critical to assessing completeness of the approach, and to evaluate appropriateness of the FM design against mission needs. Fault trees and state transition diagrams are simple visualization products. Other examples of visualization could focus on margin management, probabilistic risk assessment, or FM impacts on scenario timelines.
- Fault Management Operations Approaches: This category encompasses FM "in the loop," including algorithms, computing, state estimation / classification, machine learning, and model-based reasoning.

Advanced FM approaches may reduce the need for spacecraft safing and reliance on mission operations through more accurate health assessment, early detection of problems, more effective discrimination and understanding of root causes, or automated recovery. Particularly desirable are technologies and approaches that enable new mission concepts with greater autonomy, minimizing or eliminating spacecraft safing in response to faults – for example, riding out failures gracefully, or autonomously recovering and restarting system behavior to complete science objectives that require timely execution. Future spacecraft must be able to make decisions about how to recover from failures or degraded capacity and continue the mission, and also to work cooperatively with mission operations to replan mission goals apace with changes in system capability.

- Fault Management Verification and Validation Tools: Along with difficulties in system engineering, the challenge of V&V'ing implementations of 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.
- Fault Management 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.

Expected outcomes and objectives of this subtopic are to mature the practice of Fault Management, leading to better estimation and control of FM complexity and development costs, more flexible and effective FM designs, and accelerated infusion into future missions through advanced tools and techniques. Specific objectives include the following:

- 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, 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
- *Overall, bound and improve costs and implementation risks of FM while improving capability, such that benefits demonstrably outweigh the risks, leading to mission infusion*

ReferencesNASA's approach to Fault Management and the various needs are summarized in the NASA FM Handbook (https://www.nasa.gov/pdf/636372main_NASA-HDBK-1002_Draft.pdf). Additional information is included in the talks presented at the 2012 FM Workshop (https://www.nasa.gov/offices/oce/documents/2012_fm_workshop.html, particularly https://www.nasa.gov/pdf/637595main_day_1-brian_muirhead.pdf) Another resource is the 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). This is greatly expanded on in the following publication: Johnson, S. (ed), System Health Management with Aerospace Applications, Wiley, 2011 (
h
ttp
s://w
ww.wiley.com/en-us/System+Health+Management%3A+with+Aerospace+Applications-p-9781119998730)Fault Management Technologies are strongly associated with autonomous systems as a key component of situational awareness and system resilience. A useful overview was presented at the 2018 Science Mission Directorate

(SMD) Autonomy Workshop (https://science.nasa.gov/technology/2018-autonomy-workshop), archiving a number of talks on mission challenges and design concepts.**Expected TRL or TRL range at completion of the project:** 3 to 4**Desired Deliverables of Phase II**Prototype, Analysis, Software**Desired Deliverables Description**The aim of the Phase I project should be to demonstrate the technical feasibility of the proposed innovation and thereby bring the innovation closer to commercialization. Note, however, the R&D undertaken in Phase I is intended to have high technical risk, and so it is expected that not all projects will achieve the desired technical outcomes.The required deliverable at the end of an SBIR Phase I contract is a report that summarizes the project's technical accomplishments. As noted above, 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.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, examples, 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, and results and interpretation.

State of the Art and Critical Gaps Many recent Science Mission Directorate (SMD) missions have encountered major cost overruns and schedule slips due to difficulty in implementing, testing, and verifying FM functions. These overruns are invariably caused by a lack of understanding of FM functions at early stages in mission development, and by FM architectures that are not sufficiently transparent, verifiable, or flexible enough to provide needed isolation capability or coverage. In addition, a substantial fraction of SMD missions continue to experience failures with significant mission impact, highlighting the need for better FM understanding early in the design cycle, more comprehensive and more accurate FM techniques, and more operational flexibility in response to failures provided by better visibility into failures and system performance. Furthermore, SMD increasingly selects missions with significant operations challenges, setting expectations for FM to evolve into more capable, faster-reacting, and more reliable on-board systems.The SBIR program is an appropriate venue due to the following factors:

- Traditional FM design has plateaued, and new technology is needed to address emerging challenges. There is a clear need for collaboration and incorporation of research from outside the spaceflight community, as fielded FM technology is well behind the state of the art and failing to keep pace with desired performance and capability.
- The need for new FM approaches spans a wide range of missions, from improving operations for relatively simple orbiters to enabling entirely new concepts in challenging environments. Development of new FM technologies by SMD missions themselves is likely to produce point solutions with little opportunity for reuse and will be inefficient at best compared to a focused, disciplined research effort external to missions.
- SBIR level of effort is appropriately sized to perform intensive studies of new algorithms, new approaches, and new tools. The approach of this subtopic is to seek the right balance between sufficient reliability and cost appropriate to each mission type and associated risk posture. This is best achieved with small and targeted investigations, enabled by captured data and lessons learned from past or current missions, or through examination of knowledge capture and models of missions in formulation. Following this initial proof of concept, successful technology development efforts under this subtopic 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.

Relevance / Science TraceabilityFM technologies are applicable to all SMD missions, albeit with different emphases. Medium to large missions have very low tolerance for risk of mission failure, leading to a need for sophisticated and comprehensive fault management. Small missions, on the other hand, have a higher tolerance for risks to mission success but must be highly efficient, and are increasingly adopting autonomy and FM as a risk mitigation strategy.A few examples are provided below, although these may be generalized to a broad class of missions:Lunar Flashlight: Enable very low-cost operations and high science return from a 6U cubesat through on-board error detection and mitigation, streamlining mission operations. Provide autonomous resilience to on-board errors and disturbances that interrupt or interfere with science observations.Europa Clipper: 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.Rovers and Rotorcraft (Mars Sample Return, Dragonfly): Provide on-board capability for systems checkout, enabling lengthy drives/flights between Earth contacts and mobility after environmentally-induced anomalies (e.g., unexpected terrain interaction). Improve reliability of complex activities (e.g., navigation to features, 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).