NASA SBIR 2017 Phase I Solicitation

H6.02 Resilient Autonomous Systems

Lead Center: ARC

Participating Center(s): JPL, JSC, MSFC

Technology Area: TA4 Robotics, Telerobotics and Autonomous Systems

Future human spaceflight missions will place crews at large distances and light-time delays from Earth, requiring novel capabilities for crews with limited ground support to manage spacecraft, habitats, and supporting equipment to prevent Loss of Mission (LOM) or Loss of Crew (LOC) over extended duration missions. In particular, these capabilities are needed to handle faults leading to loss of critical function or unexpected expenditure of consumables. Expanded flight control functionality will be on-board spacecraft to support autonomy with significant automation, autonomy, and decision support software. The increasingly complex interconnectivity of these elements introduces new vulnerabilities within space systems that are sometimes impossible to predict. In that context, one key property of the respective system is its resilience to unforeseen events.

Resilience, as defined by the U.S. National Academy of Sciences [1] (NAS), is the ability to plan and prepare for, absorb, recover from, and more successfully adapt to adverse events. Within this definition, resilience has two manifestations: engineering and ecological. Engineering resilience is focused on the ability of a system to absorb and recover from adverse events, while ecological resilience is focused on understanding how close a system is to collapse and reorganization. The engineering definition brings resilience principles such as robustness, redundancy, and modularity, while the ecological definition supports principles of flexibility, adaptability, and resourcefulness.

To enable resilient behavior of a system (such as a vehicle, a habitat, a rover, etc.), "resilience" needs to be built-in during the design phase of the system development. To that end, the operational states of a system’s component need to be considered in conjunction with the intended function of the component and its possible failure modes throughout the vehicle's life cycle. Where possible, critical failures are eliminated during the design stage. For failure modes that cannot be eliminated, a mechanism needs to be designed that considers how to have optimal state awareness during operations and to mitigate the fault. Mitigation can be accomplished through fault avoidance, fault masking, or Fault Detection, Assessment, and Recovery (FDIR). FDIR can be realized through hardware or software solutions as well as by intervention of the mission crew or mission control. The detection / assessment / recovery process will involve identification of:

- Small variations in overall system performance that may “coincide and combine” to produce significant risk.
- Dependencies within the system that contribute to unforeseen increased risk.
- The strategies and solutions used by crew and controllers to run mission operations safely.
- Recovery/fallback mechanisms that help the human/technology system cope with foreseen and unforeseen operational conditions and events.
- The adaptability and flexibility needed to handle unpredictable and uncertain situations.
- The different technical, functional, and procedural features that can interact in a positive way to achieve

mission success.

Four processes characterize the emergence of resilience as a system property:

- *Sensing* - measuring new information about a system's operating environment with focus on anomalous data. These data can alert system evaluators of overlooked possibilities. This process connects components in the physical domain to the information domain.
- *Anticipation* - imagining multiple future states without reducing improbability to impossibility; this includes incorporating the uncertainty in the future states and including the impact of such uncertainty on system operation. This process connects components in the information domain to the cognitive domain.
- *Adaptation* - reacting to changing conditions or uncertain states to restore critical functionality under altered conditions or operating environments. This process connects the cognitive domain to the physical domain.
- *Learning* - observing external conditions and system responses to improve understanding of relationships and possible futures, identifying needs for system improvement where applicable. This process links the physical, information, and cognitive domains together and can incorporate the social or human crew domain depending on the system studied.

Since a vehicle is made up of many components, a system-of-system's approach needs to be considered in a multi-objective optimization context to account for interdependencies and to realize possible mutually beneficial mitigation solutions for resiliency.

Proposals to this subtopic should specify innovation and approaches toward two goals:

- Development of methods and tools that allow the assessment and optimization of system resilience during its conceptual design stage, while simultaneously maximizing reliability and safety.
- Development of measures and metrics that quantify the degree of resilience of a system with respect to a mission ConOps and hazard analysis.

Resilience measures and metrics must be general enough to support broad applications, yet precise enough to measure system-specific qualities. Such metrics are necessary to make resource and operations decisions. Risk metrics tend to assess risks to individual components, ignoring system functionality as the result of interacting components. Resilience measures and metrics also need to account for uncertainty in the planned operation of the system, and focus on integrating statistical methods for uncertainty propagation into resilience-based design. Rather than the static view of systems and networks in risk assessment, resilience adopts a dynamic view. This means resilience metrics must also consider the ability of a system to plan, prepare, and adapt as adverse events occur, rather than focus entirely on threat prevention and mitigation. Finally, resilience depends upon specific qualities that risk assessment cannot quantify, such as system flexibility and interconnectedness.

Proposed solutions are expected to have characteristics including (but not limited to):

- Life-cycle models (i.e., models that assess the resilience of the system over its entire life-cycle) that encapsulate cost/benefit of envisioned design solution and that can be used to inform about the resilience of the system.
    - Models may need to be built at the appropriate fidelity level to capture relevant fault behavior.
    - Models may need to assess behavior and consequences during degraded (or faulted) state.
    - Models should also be able to assess mitigation actions that are part of an integrated health management approach.
- Design optimization methodology that can systematically incorporate health management solutions.
    - Methods that integrate optimal decision-making into the design concept.
    - Methods that make use of both system health models and observations to provide the best decision given the information available.
    - Methodology to allow bi-directional exchange between a model and the analysis tool.
    - Methods that systemically include desired levels of resilience in the design optimization process.
- Uncertainty management.

    - Identify the various sources of uncertainty that affect system performance, and quantify their combined effect on both system failure and resilience.
    - Systematically incorporate uncertainty in the design process, thereby incorporating both resilience and likelihood of failure directly during the design stage.

This SBIR work aims to generate a practical toolkit for space systems that can deliver solutions with assured levels of performance, reliability and resilience, while accommodating: uncertainty; incomplete knowledge; sparsity, or high volumes, of data; and humans in the loop.

Metrics for success include:

- Development of generic quantitative measures and metrics that evaluate system resilience, and their application to space relevant systems or subsystems.
- Demonstrated improvement of resilience over baseline design for at least two different space relevant systems or subsystems.
- Consideration of at least 3 different fault modes.
- Software tools must be able to accept other systems or subsystems through appropriate interface.

SBIR work is expected to deliver mainly software in the form of tools used during the design stage and also prototype software that would manage resiliency during autonomous operations. For the latter, the SBIR effort should analyze sensors, computational hardware, and software stack:

- Resiliency for the computational system should also be addressed.
- In-space applications are preferred, but terrestrial analogues will be considered.

Proposals must demonstrate mission operations risk reduction through appropriate metrics;

Deliverables: tools developed, algorithms and any data generated in simulations or experiments.

Below are a few links to documents on resilience that may be useful to understand the context:

- Resilience Engineering and Quantification for Sustainable Systems Development and Assessment: Socio-technical Systems and Critical Infrastructure: https://www.irgc.org/wp-content/uploads/2016/04/Haering-et-al.-Resilience-Engineering-and-Quantification.pdf.
- The New Resilience Paradigm - Essential Strategies for a Changing Risk Landscape: https://www.irgc.org/wp-content/uploads/2016/04/Fiksel-The-New-Resilience-Paradigm.pdf.

References:

Kash Barker, Jose Emmanuel Ramirez-Marquez, Claudio M. Rocco, “Resilience-based network component importance measures”, Reliability Engineering and System Safety 117 (2013) pp.89–97.

Daniel A. Eisenberg, Igor Linkov, Jeryang Park, Matthew E. Bates, Cate Fox-Lent, Thomas P. Seager, Resilience Metrics: Lessons from Military Doctrines: http://www.thesolutionsjournal.org/node/237200.

[1] Committee on Increasing National Resilience to Hazards and Disasters; Committee on Science, Engineering, and Public Policy (COSEPUP); Policy and Global Affairs (PGA); The National Academies. . Disaster Resilience: A National Imperative: http://www.nap.edu/catalog.php?record_id=13457. The National Academies Press. (2012).