SERC DOCTORAL STUDENT FORUM 2023 | NOVEMBER 14, 2023

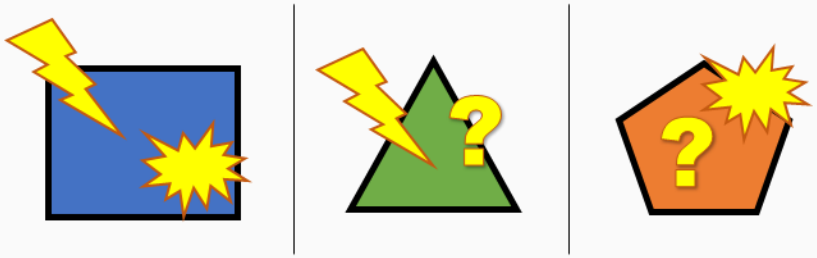
A State-based Probabilistic Risk Assessment Framework for System-of-systems Operations

Sonali Sinha Roy

PURDUE UNIVERSITY

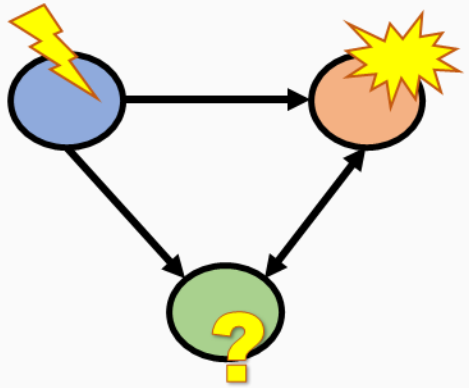
Background

- System of systems (SoS): Collection of systems that can be operated and managed independently while serving a common goal.
- System-level risks, failure modes, and uncertainties can affect the entire SoS (or mission) → Risk assessment of SoS operations (missions) becomes complicated.
- Traditional risk analysis practices:



Detailed risk analysis for individual systems

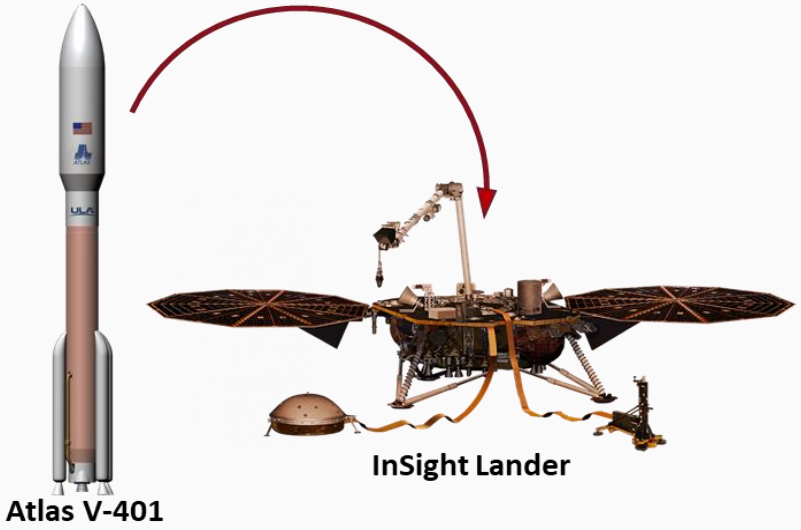
+



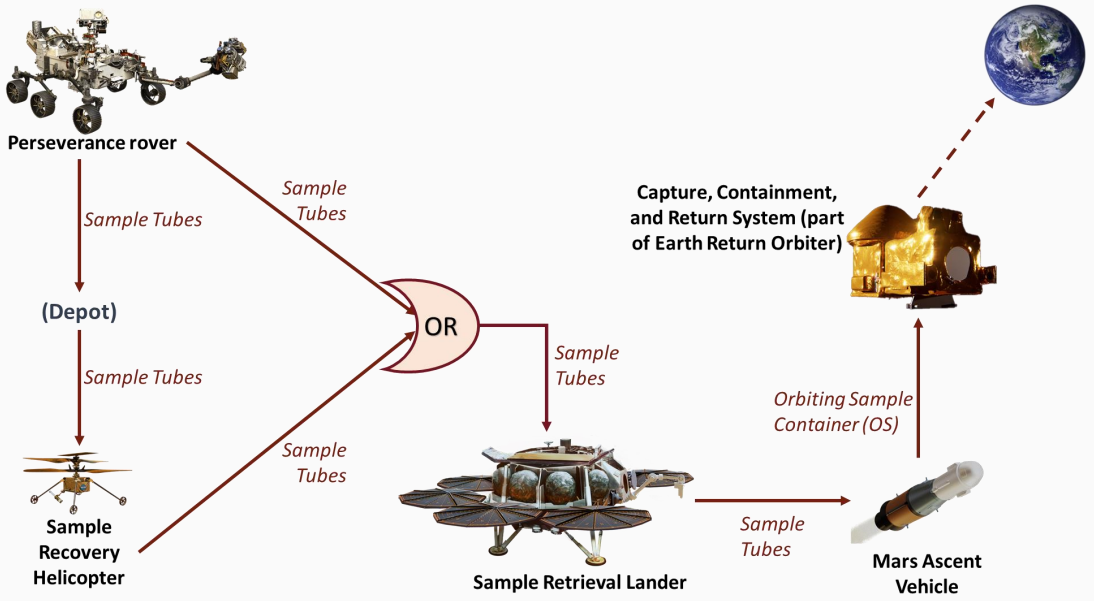
SoS/mission analysis with simplified versions of the constituent systems and their interactions

Motivation

- SoS missions are changing → Systems now interact more deeply and work in tandem to fulfil the mission objectives.



Mars InSight Mission



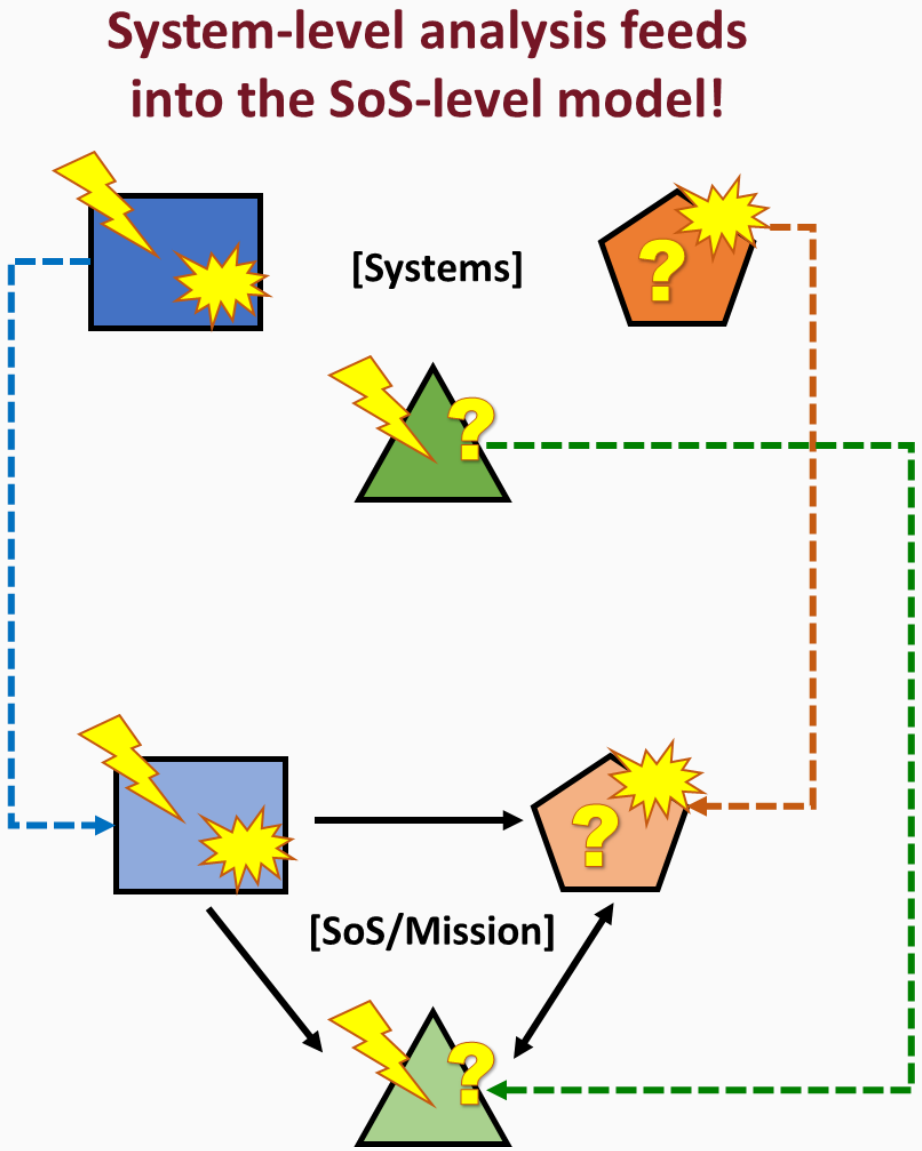
Mars Sample Return Program

- Traditional risk assessment methods are no longer adequate for complex, multi-system missions!
- Mission analysis models must include operational nuances of the constituent systems.

Research Goals

To develop a risk analysis method that can

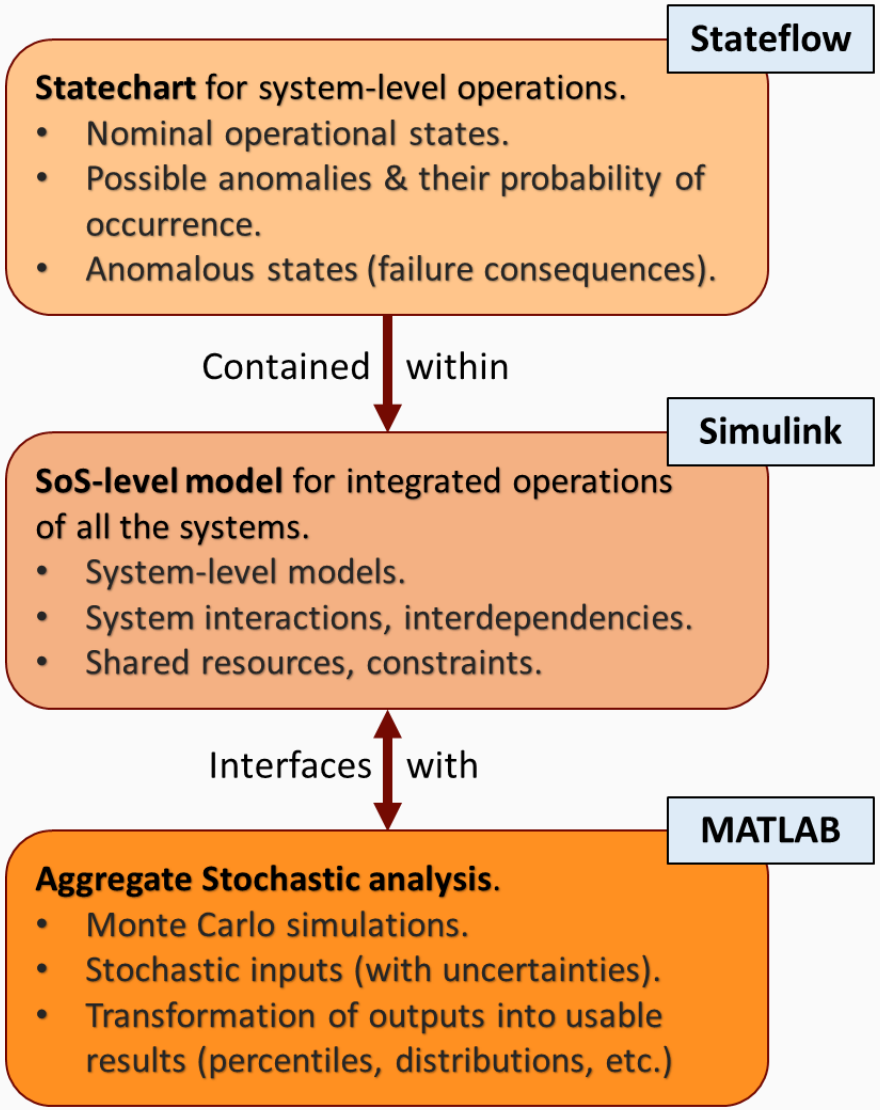
- Include the system-level operations and operational risks in the SoS/mission-level models.
- Observe and analyze the interaction between the SoS/mission and its constituent systems.
  - How does the mission's architecture and objectives affect system-level operations?
  - How do system-level risks and uncertainties affect the mission outcomes?



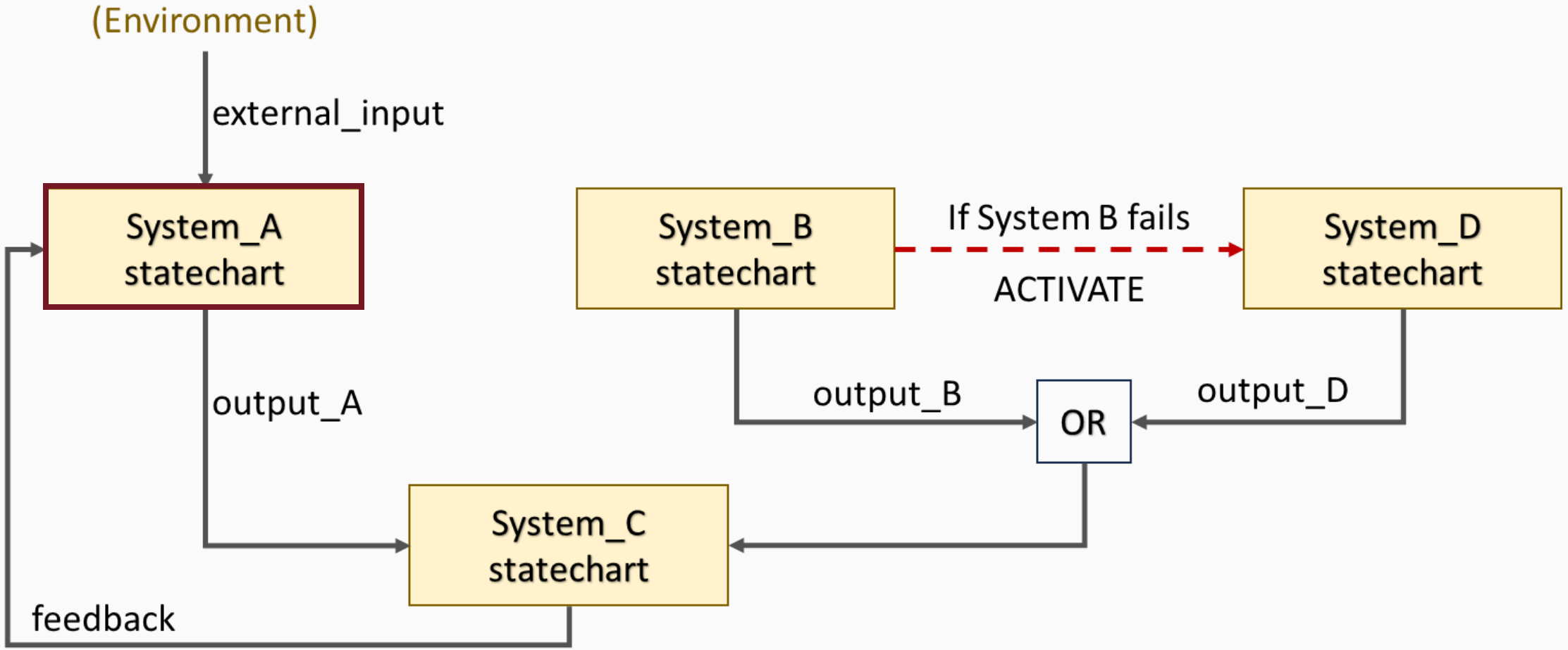
Technical Approach: State-based PRA Framework

State-based Probabilistic Risk Assessment (PRA) Framework

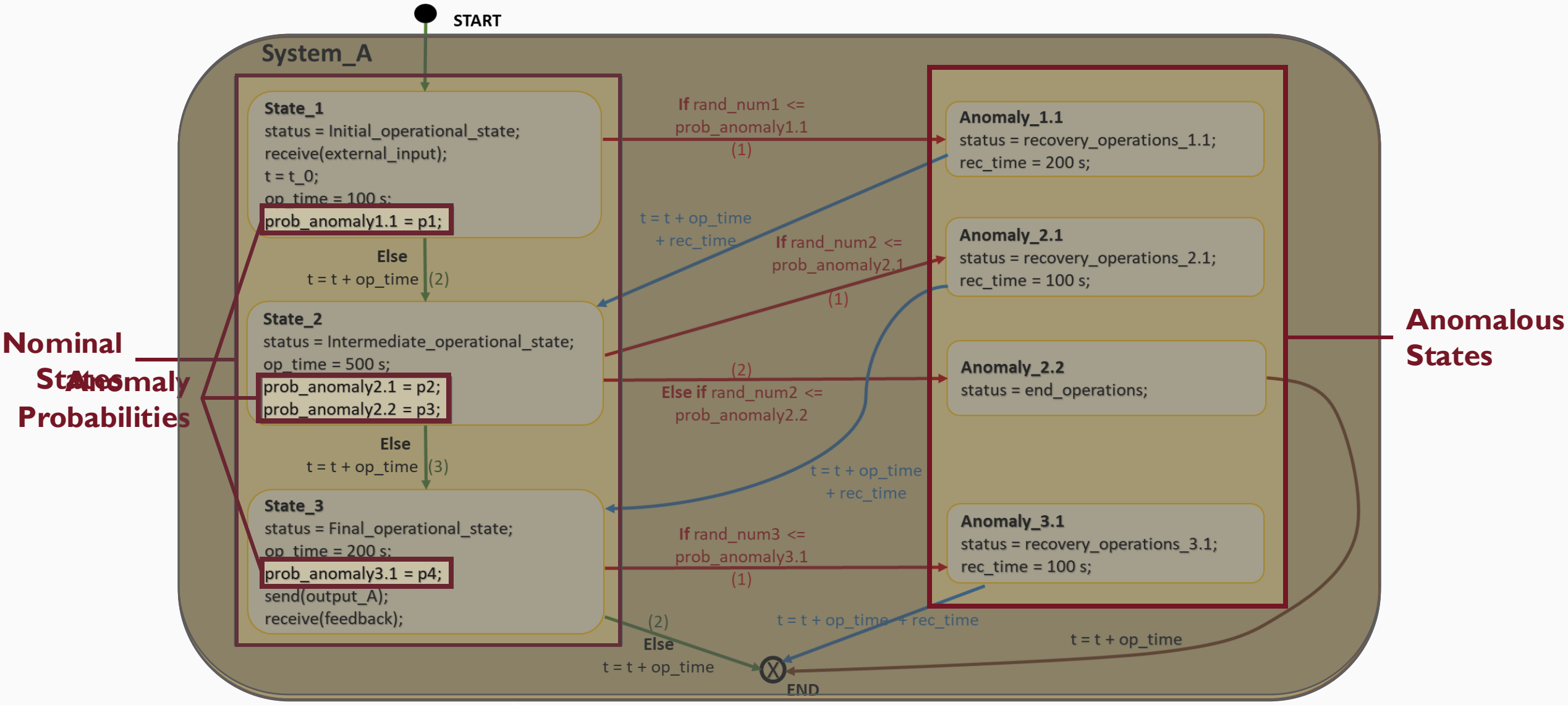
- Consists of three parts:
  - System-level statecharts
  - SoS-level model
  - Aggregate stochastic analysis
- Composite model (system-level + SoS-level) helps in understanding and analyzing the relationship between the SoS (or mission) and its constituent systems.
- SoS-level impact of system-level risks, their compound and cascading effects, and the effect of stochasticity and uncertainties can be assessed.



Mission/SoS-level Model



System-Level Statechart



Demonstration: Mars Sample Return (MSR) Program

Perseverance rover

Sample Tubes

(Depot)

Sample Tubes

Sample Recovery Helicopter

Sample Tubes

Sample Tubes

OR

Sample Tubes

Sample Retrieval Lander

Sample Tubes

Mars Ascent Vehicle

Orbiting Sample Container (OS)

Capture, Containment, and Return System (part of Earth Return Orbiter)

Application of the Framework

Stateflow

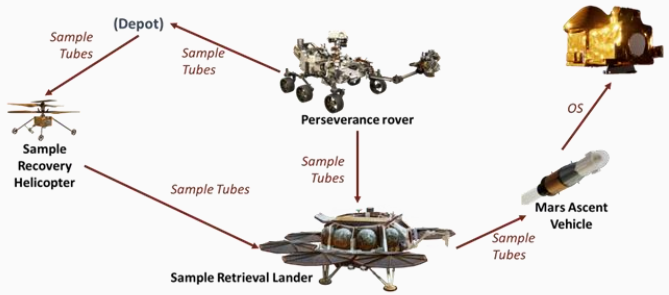
Statechart for system-level operations.
- Nominal operational states.
- Possible anomalies & their probability of occurrence.
- Anomalous states (failure consequences).

How does each system operate?
In what ways can the systems fail?

Contained within

Simulink

SoS-level model for integrated operations of all the systems.
- System-level models.
- System interactions, interdependencies.
- Shared resources, constraints.



How do all the systems interact within the SoS?
How do they affect the SoS operations?

Interfaces with

MATLAB

Aggregate Stochastic analysis.
- Monte Carlo simulations.
- Stochastic inputs (with uncertainties).
- Transformation of outputs into usable results (percentiles, distributions, etc.)

What are the most critical failure modes?
What are the main sources of operational delays?
How do different types of system-level failures affect the SoS-level performance?

MSR Systems – Nominal States and Failure Modes (1)

System	State	Nominal window	Anomalies	Probability of occurrence	Mitigation/Consequence
Perseverance	Move to SRL	10 sols	Rover immobile	1%	Collect depot samples using SRH
			Rover stuck	5%	Recover mobility – 2 sols
	Drop samples in workspace	5 sols	Sample drop off mechanism malfunction	3%	Not all samples dropped (success ratio → from uniform distribution)
SRL (including STA)	Land	--	Crash	1%	End mission
	Deploy STA	1 sol	Deployment failure	2%	End mission
	Collect sample tubes (i.e, pick up tubes, place in OS)	5 sols	Sample collection failure	5%	Not all retrieved samples are placed in OS (success ratio → from uniform distribution)
SRH	Fly	2 sols / sample	Crash	1%	Helicopter stops operating (x 2 = end mission)
			Navigation issue	5%	Recover localization - Delay 5 sols
	Handle tube	2 sols / sample	System malfunction	3%	Recovery – 2 sols delay

MSR Systems – Nominal States and Failure Modes (2)

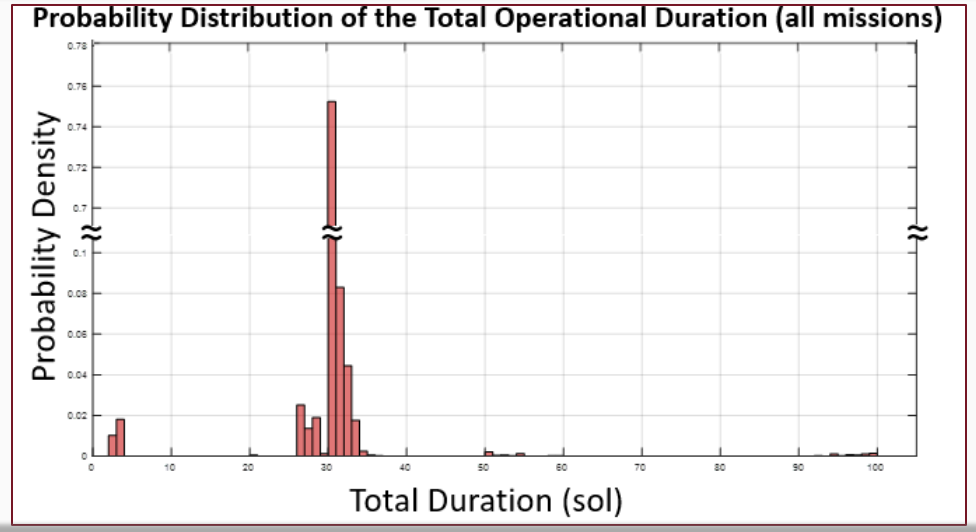
System	State	Nominal window	Anomalies	Probability of occurrence	Mitigation/Consequence
MAV	Launch preparation	5 sols	Release mechanism failure	3%	End mission
			Positioning error	5%	Reposition or trajectory correction during launch; additional 1 sol
	Launch to Orbit	1 sol	Launch failure	2%	End mission
	Release OS	1 sol	Release mechanism stuck	5%	Delay (1 sol) until unstuck
			Incorrect OS orbital release	2%	End mission
CCRS	OS detection	2 sols	Detection error	5%	Additional 2 sols for correct detection
	OS capture	1 sol	Capture or containment failure	4%	End mission

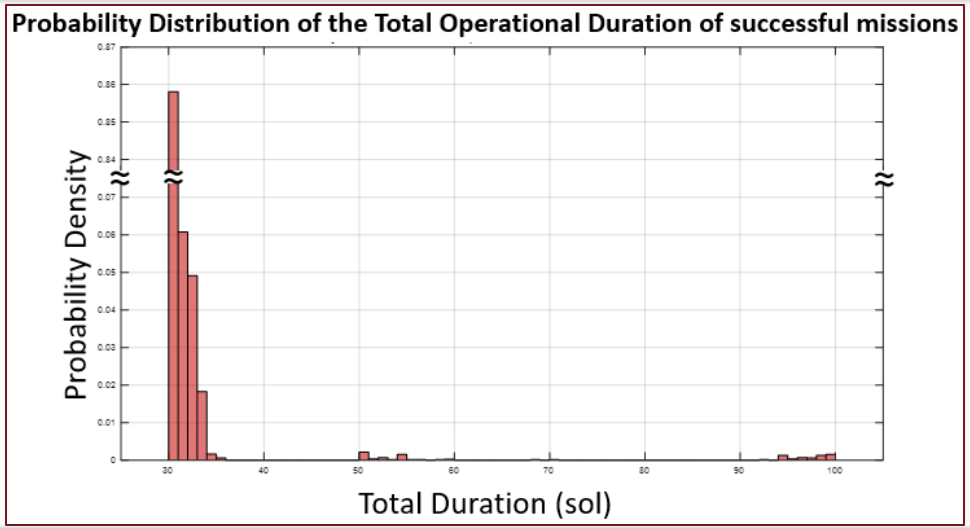
Examples of Results (1): SoS Mission Statistics

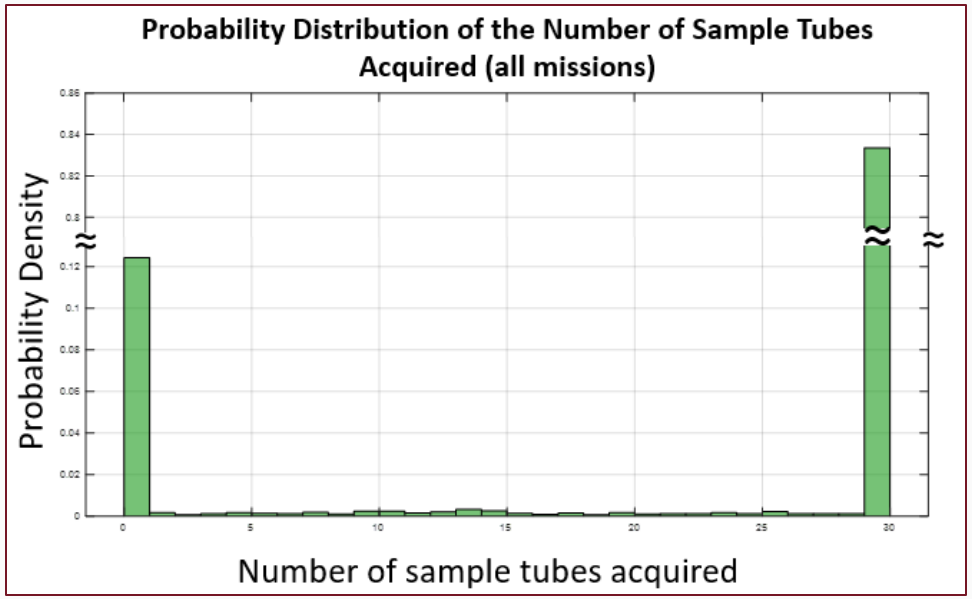
Performance Metric	Mean	Standard Deviation	Minimum	Maximum	99th Percentile
Total operational duration (sol)	29.00	8.50	0	100	50
Number of sample tubes acquired	24.93	10.93	0	30	30

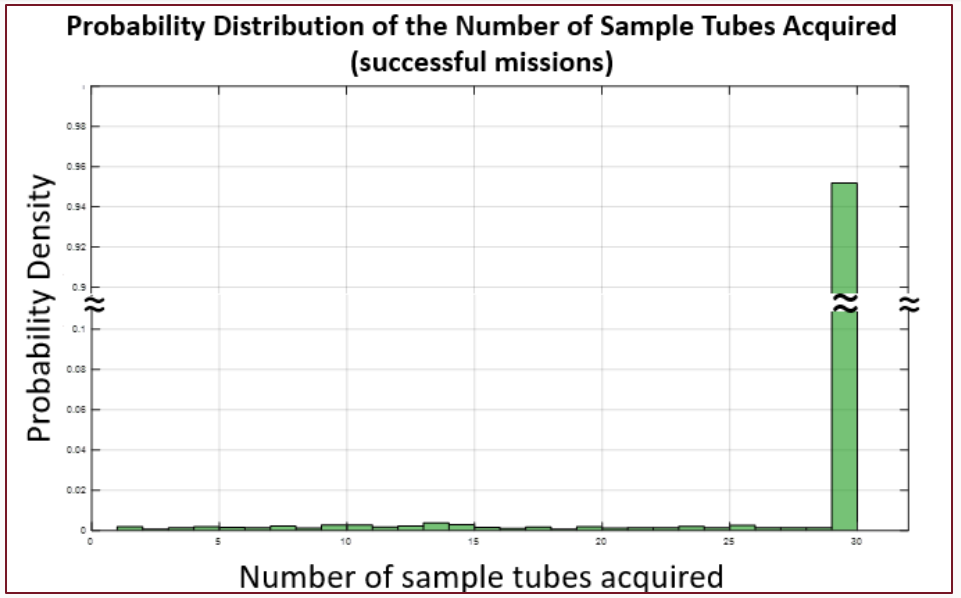
- Expected duration and the expected number of samples acquired? This can be used to determine the mission success criterion.
- 99th percentile value of the duration can help in mission scheduling.
- Statistics can be compared for different architectures to select the most feasible one.

Examples of Results (2): Distribution of Performance Metrics

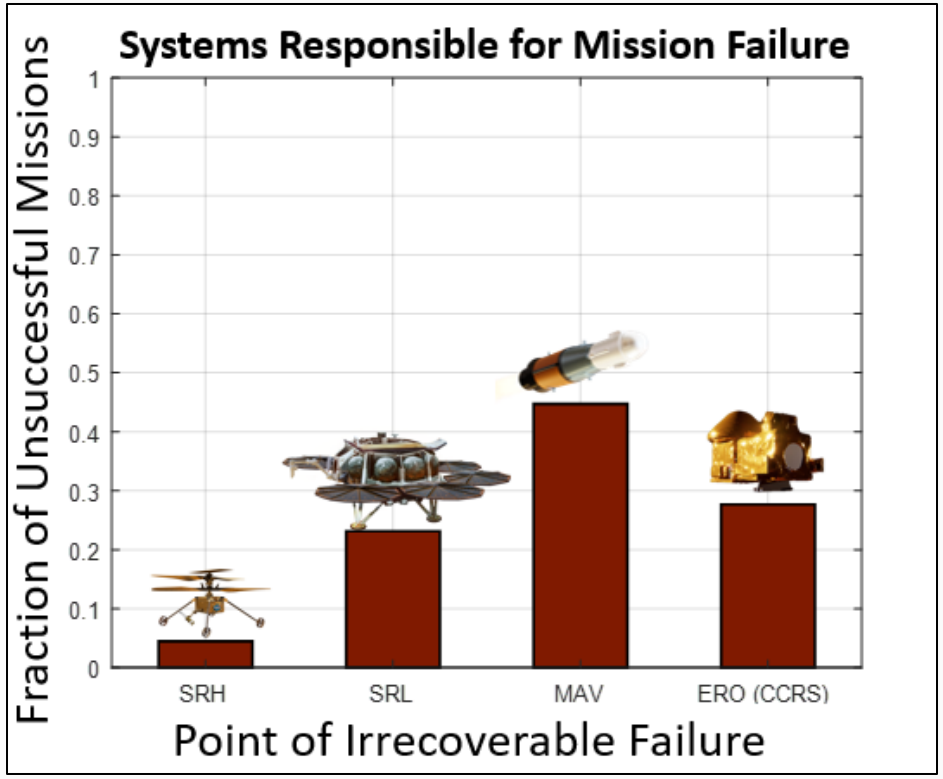








Examples of Results (3): Failure Susceptibilities and Critical Risks



- What systems need to be improved to boost the mission success probability?
- Where are backups and redundancies needed?

Research Contributions

This framework is aimed at contributing to the field of SoS risk assessment in the following ways:

- Integration of the operations of interdependent systems into a cohesive mission.
- Multi-faceted risk analysis of the SoS/mission while considering system-level risks and uncertainties.
- Analysis of SoS operations or missions at various levels of hierarchy.
- Interpretation of the SoS mission as an emergent outcome of the interactions among constituent systems.

Applications

- Mission analysis and mission assurance
  - Helps establish and analyze the trade space.
  - Not constrained by a “binary” definition of mission success or failure.
  - Data can be used for benchmarking or cost vs. benefit analysis in later stages.
- Sensitivity analysis and architecture selection
  - Mission-level performance metrics can be compared for different operational concepts and various types of uncertainties in the inputs.
  - Helps in identifying the impact of uncertainties and selecting feasible operational concepts and architectures.
- Critical mission risks
  - Highlights the areas where further development may be necessary.
  - Informs the decision-making process at the managerial level – can guide funding and resource allocation.

Future Work and Acknowledgment

- Addition of an optimization module that analyzes the results of various architectures and identifies the most optimal one, based on a set of SoS-level performance parameters.
- Expansion of Mars Sample Return application:
  - Multi-disciplinary optimization of the science return value (a function of the number of samples and sample diversity), mission duration/timeline, and technical risk.
  - This will allow us to select the best sampling locations, the ideal landing spot for the Sample Retrieval Lander, and best strategy to deliver samples to the lander.
- This framework was originally developed as a part of a project sponsored by NASA JPL. Our team would like to thank JPL for its support and guidance during the development of this framework.

Key References

1. Kaplan, S., & Garrick, B. J. (1981). On The Quantitative Definition of Risk. *Risk Analysis*, 11-27.
2. Stamatelatos, M., & Dezfuli, H. (2011). *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners.* NASA.
3. Darpel, S., Beckman, S., Ferlin, T., Havenhill, M., Parrot, E., & Harcula, K. (2020). Method for tracking and communicating aggregate risk through the use of model-based systems engineering (MBSE) tools. *Journal of Space Safety Engineering, 7*(1), 11-17.
4. Nejad, H. S., Parhizkar, T., & Mosleh, A. (2022). Automatic generation of event sequence diagrams for guiding Simulation based dynamic probabilistic risk assessment (SIMPRA) of complex systems. *Reliability Engineering & System Safety, 222*, 108416.
6. McCoy, K., Everline, C., & Bendig, J. (2019). *Model-based Probabilistic Risk Assessments (PRA)*. NASA.
7. NASA. (2022). Mars Sample Return. Retrieved from NASA: https://mars.nasa.gov/msr/

Thank you

Stay connected with SERC Online:

Email the presenter: Sonali Sinha Roy

ssinhar@purdue.edu

Email the advisor: Dr. Daniel DeLaurentis

ddelaure@purdue.edu