| galois |

Uniting hierarchical planning and model-based systems engineering to automate failure recovery planning

Tyler Smith
tyler@galois.com

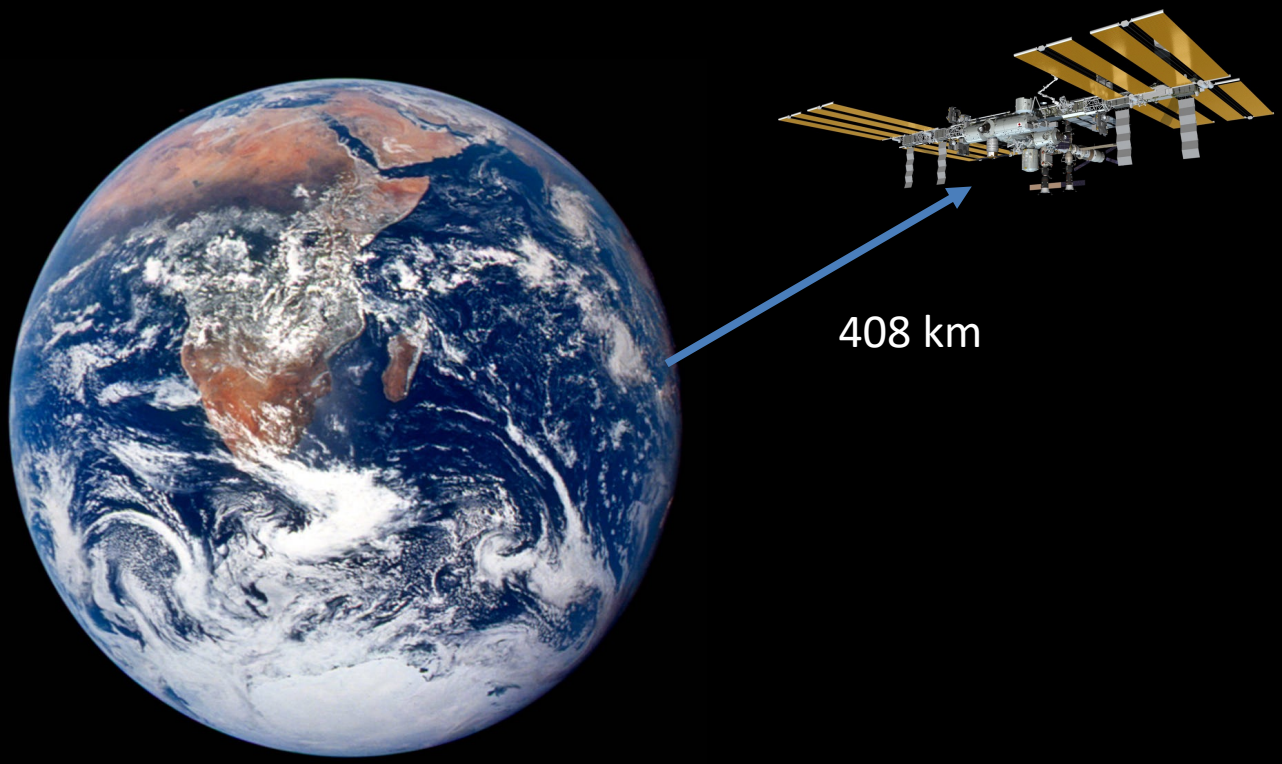
galois

Bottom Line Up Front

Automated generation of failure recovery plans is possible, mission rules and goals provide necessary structure.

Complexity and Autonomy

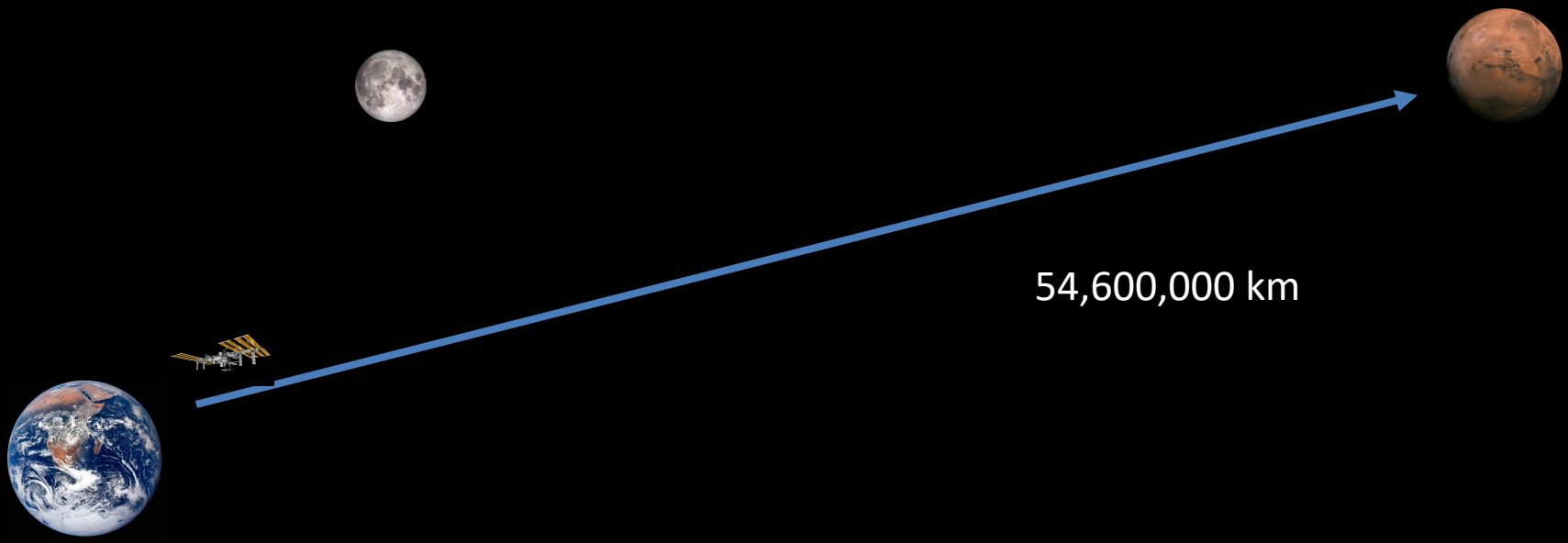
Crewed and uncrewed aerospace systems are increasing in complexity and decreasing in reliance on ground-based operators.



Source Source

384,000 km

Source

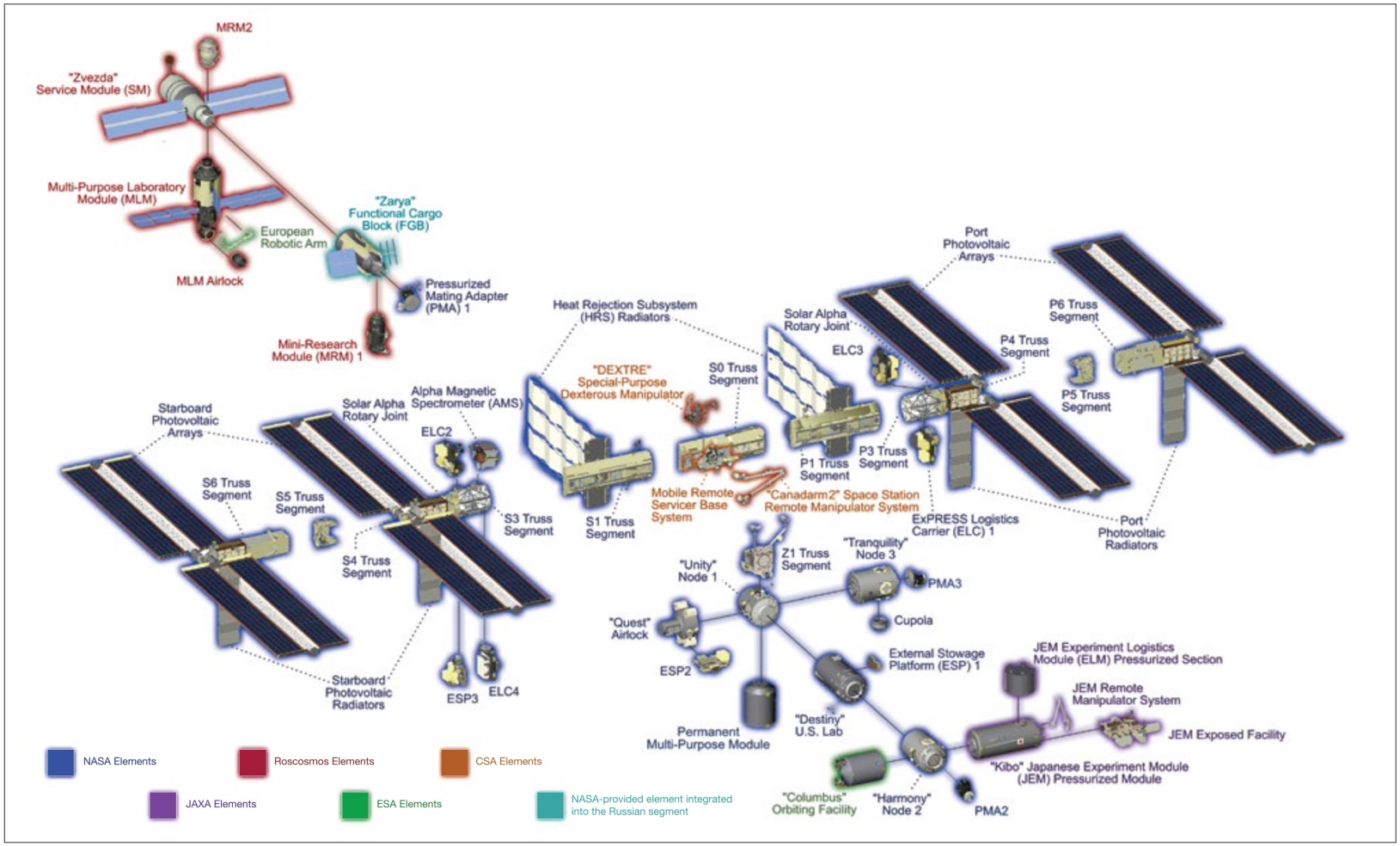


Source

System Configuration Changes(verb)

Missions that include multiple system configuration changes or extensions are a major piece of the National Aeronautics and Space Administration (NASA) roadmap for the coming decades.

The international space station was been assembled over two decades of missions, and is still evolving.



Source

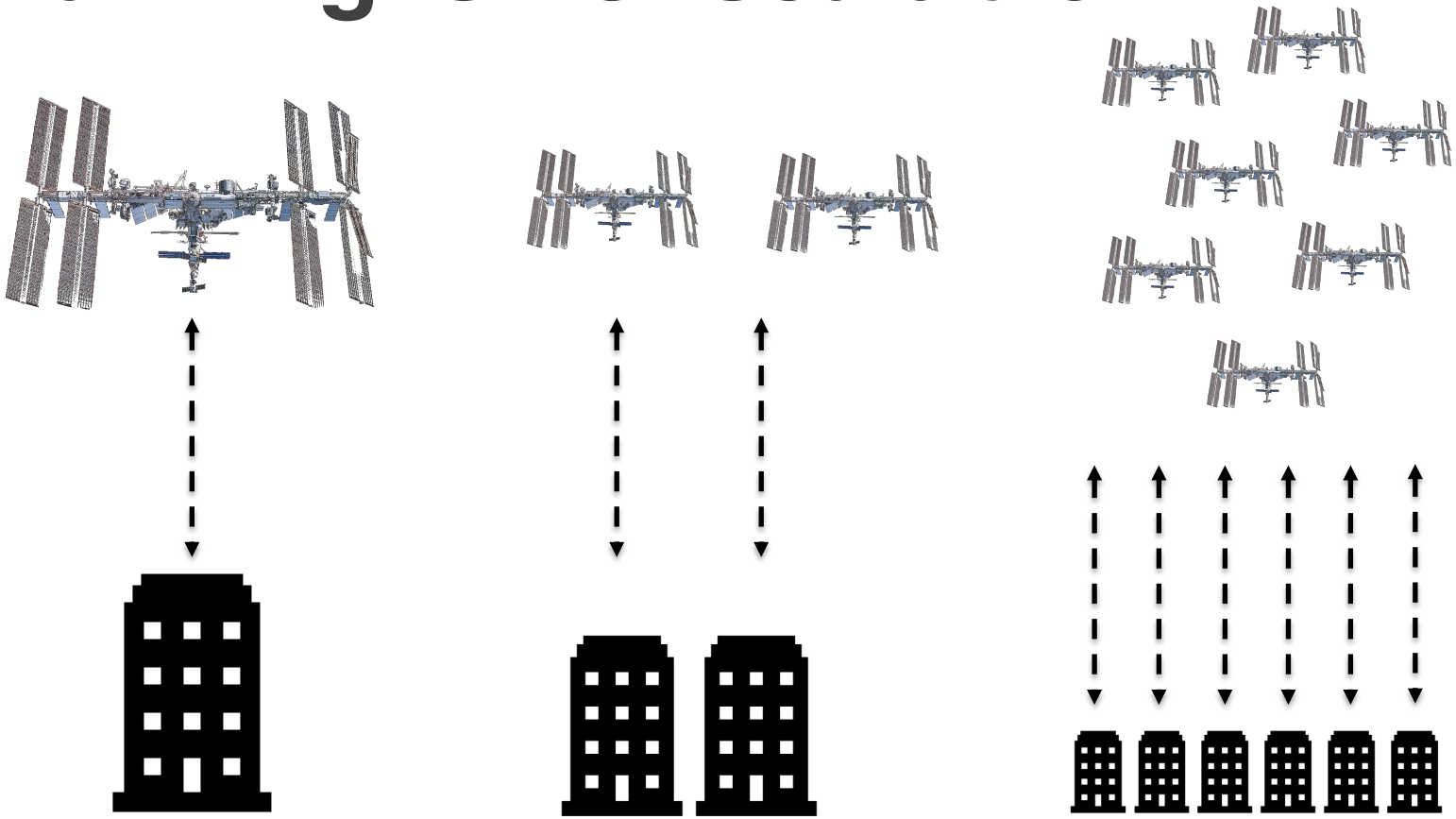
The Artemis program will assemble components on the lunar surface and in lunar orbit (Gateway).

Source

Failure Recovery Planning Today

1. Go to Safe Mode → Phone Home
2. Execute pre-planned recovery procedure

Manual Failure Recovery Planning is not scalable



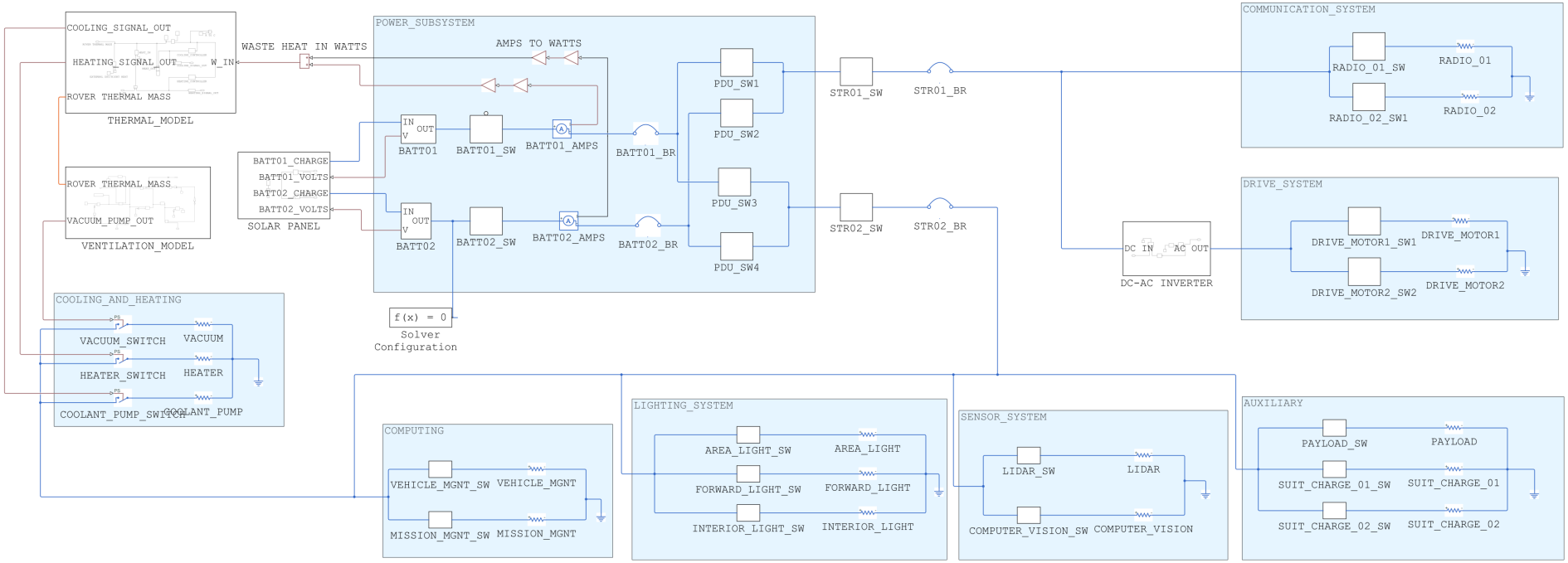
Automation can help reduce operational costs and keep error rates low.

Photo Source

What do we do?

1. Maintain a model of the system
2. Formalize mission objectives and rules
3. Use the model as the basis for automated planning

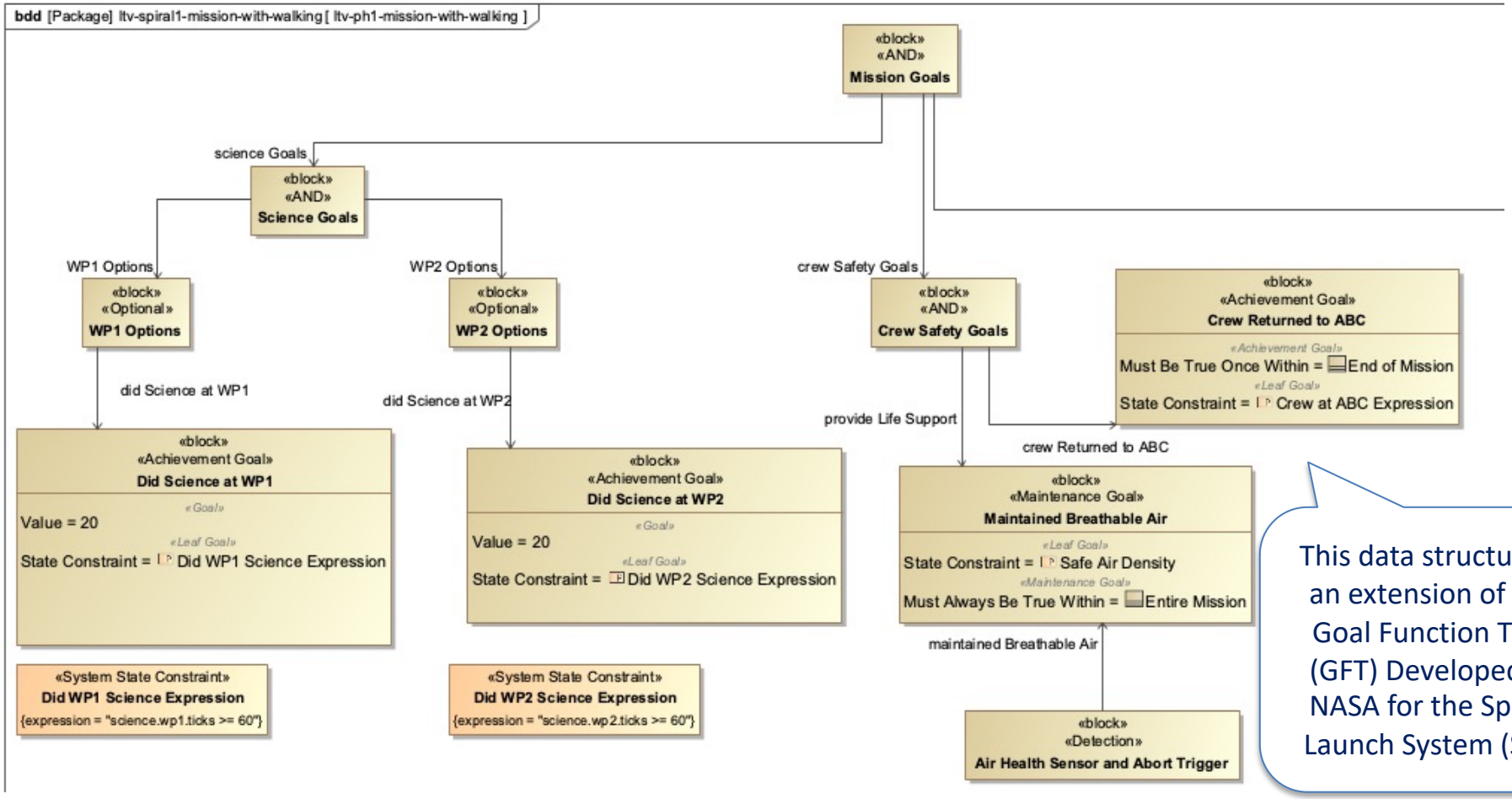
Maintain a Model of ~~the~~ each System



When the system changes (or will change) keep the model updated (it's a digital twin!)

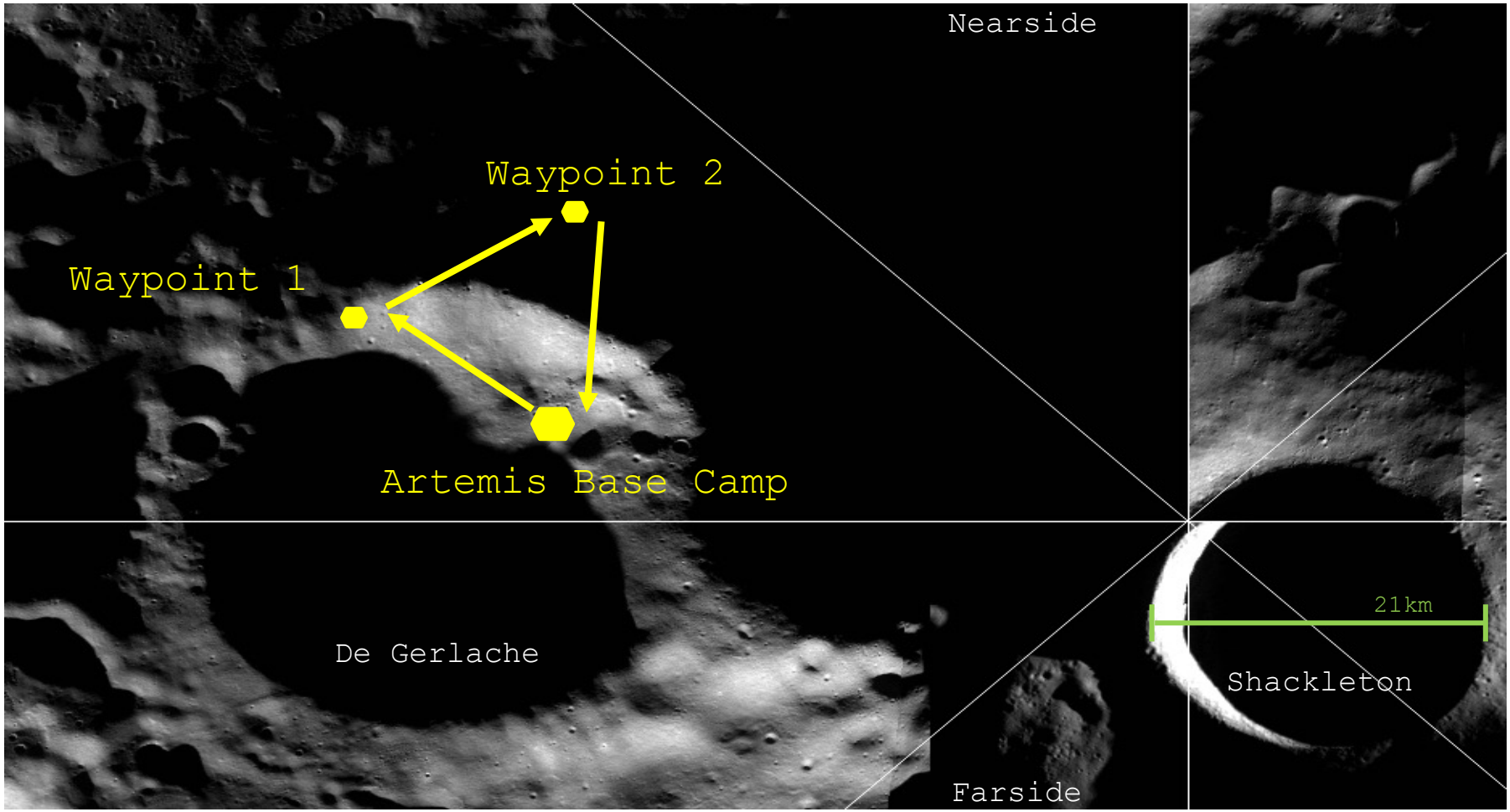
Mathworks Simscape

Formalize Mission Objectives and Rules



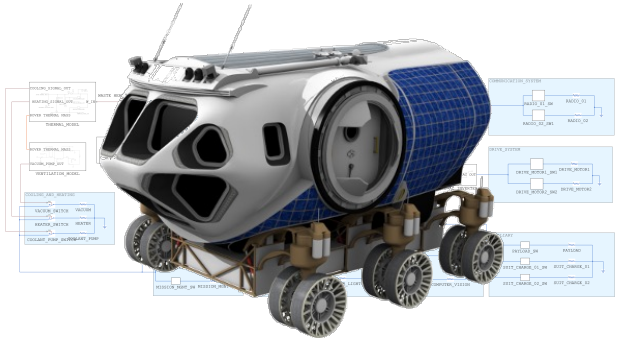
This data structure is an extension of the Goal Function Tree (GFT) Developed at NASA for the Space Launch System (SLS)

Example Mission



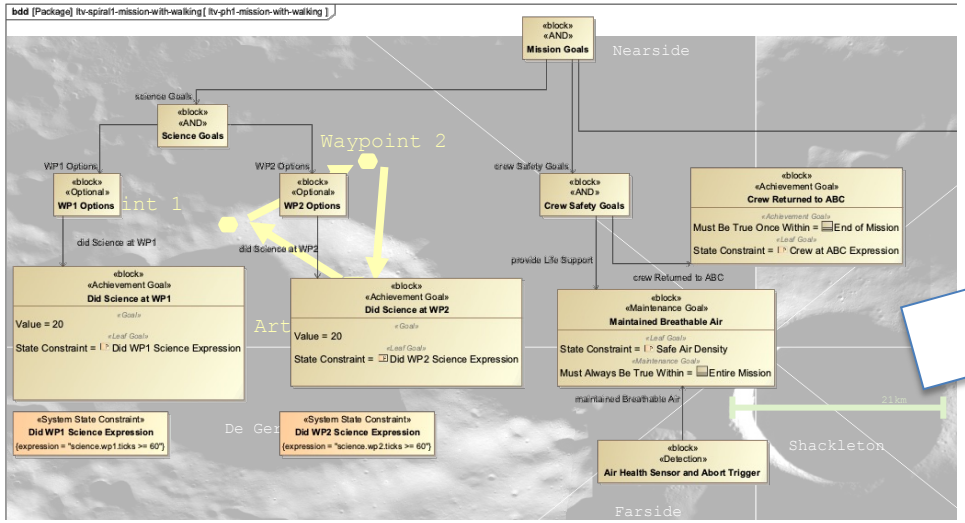
Lunar Surface Source

Use the Models as a Basis for Automated Planning



What could go wrong?

What the System *can* do



What the System *must* do

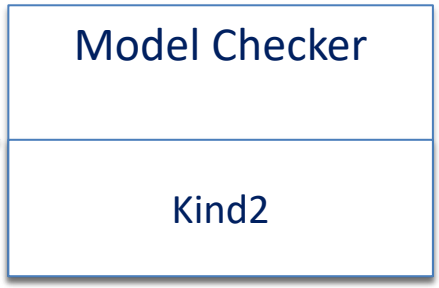
Composite Formal Specification

Lustre Model of System Behavior and Mission Constraints

Rover Source
Lunar Surface Source

Put the Pieces Together

Analyze the Composite Formal Specification with Kind2



Tick	Action	Variable Value
0	Request Forward	control.dir : forward
8	Request Stop	control.dir : stop
11	Request Reverse	control.dir : reverse

Kind2 generates a "counterexample" which is the procedure

Conclusion

Automated generation of failure recovery plans is possible, mission rules and goals provide necessary structure.