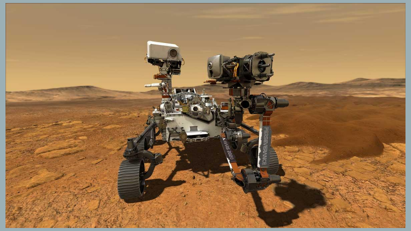
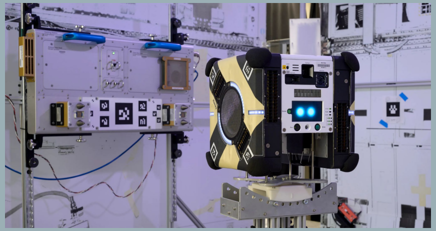
LTL PATTERNS FOR AUTONOMOUS SPACE ROBOTICS

Mahdi Etumi
Hazel M. Taylor
Marie Farrell



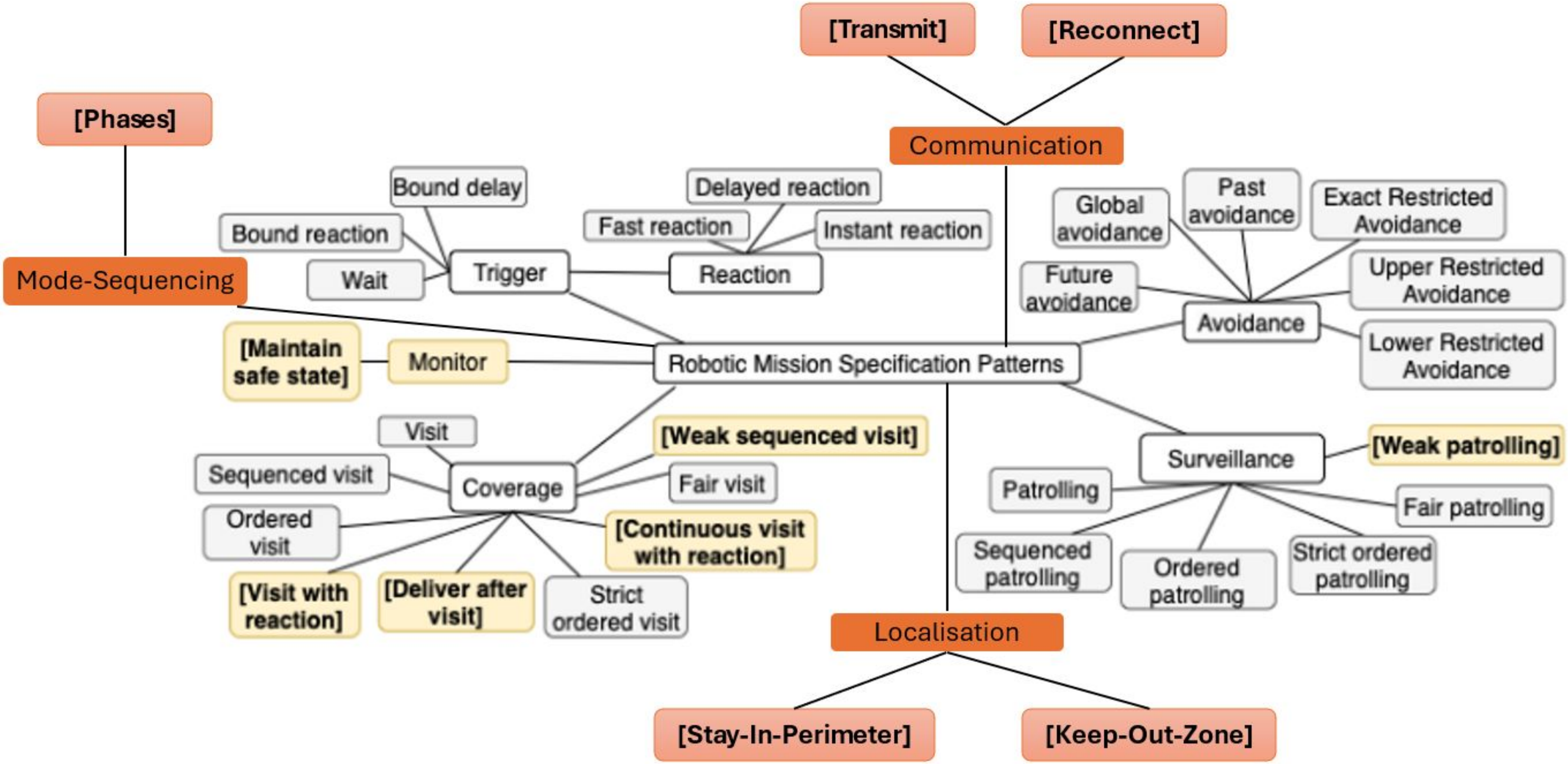


INTRO

- **Aim:** Identify patterns for autonomous space robotics
- **Methodology:**
    - Literature review of existing space missions
    - We used FRET to help with formalisation
- **Results:**
    - 120 requirements were found
    - 5 new specification patterns were derived

INTERVIEW STRUCTURE

- We will show you the patterns
- We will ask you some questions
- This will take no longer than an hour



[Transmit]

[Reconnect]

Communication

[Phases]

Mode-Sequencing

Bound delay

Bound reaction

Wait

Trigger

Delayed reaction

Fast reaction

Instant reaction

Reaction

Global avoidance

Past avoidance

Exact Restricted Avoidance

Future avoidance

Upper Restricted Avoidance

Avoidance

Lower Restricted Avoidance

[Maintain safe state]

Monitor

Robotic Mission Specification Patterns

Visit

Sequenced visit

Coverage

[Weak sequenced visit]

Fair visit

Ordered visit

[Continuous visit with reaction]

[Visit with reaction]

[Deliver after visit]

Strict ordered visit

Surveillance

[Weak patrolling]

Patrolling

Fair patrolling

Sequenced patrolling

Ordered patrolling

Strict ordered patrolling

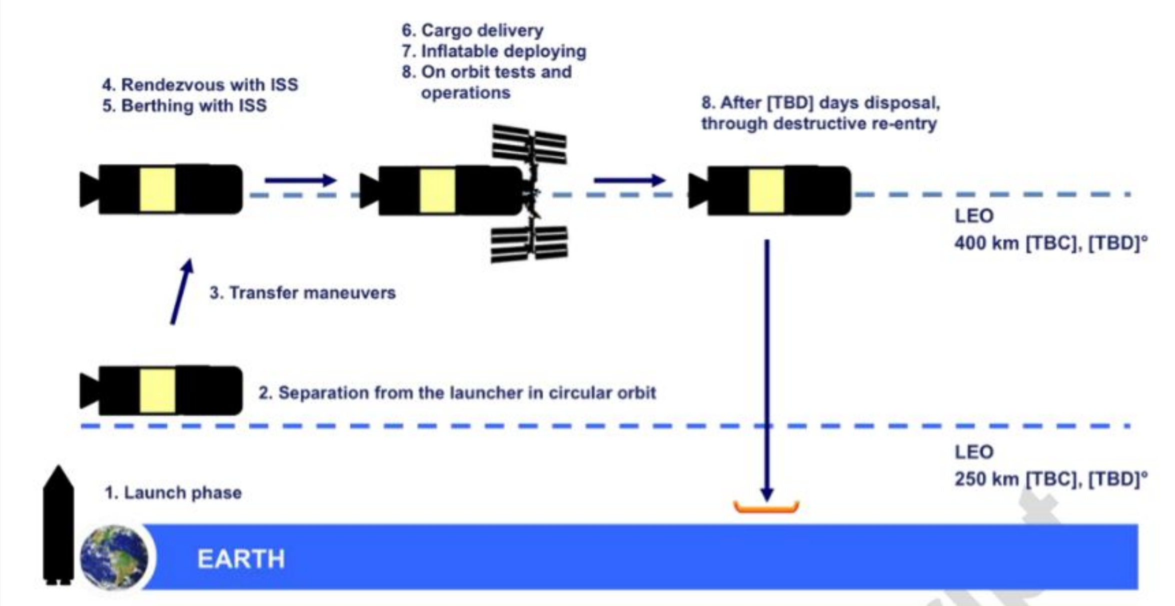
Localisation

[Stay-In-Perimeter]

[Keep-Out-Zone]

PATTERN 1: PHASES

- One recurring pattern was the sequencing of phases
- Phases represent the different stages that a system may be at, during operation
- It specifies that higher level requirements such as phases or steps flow correctly one after the other



PATTERN STRUCTURE: PHASES

- Let p1, p2 be system phases and c1, c2 be conditions

Whenever p1 system shall eventually satisfy c1

Whenever c1 system shall at the next timepoint satisfy p2

Whenever p2 system shall eventually satisfy c2

$$p_1 \Rightarrow F(c_1 \Rightarrow X(p_2 \Rightarrow F(\ldots F(c_{n-1} \Rightarrow X(p_n)))))$$

EXAMPLE

- *“The launch phase begins with lift-off and ends at burn out. The Separation phase begins with burn out, leading to transfer orbit insertion. During transfer, the spacecraft moves toward the Cygnus arrival near the ISS. Finally, the rendezvous phase covers the approach and capture by the robotic arm.”*

Whenever LaunchPhase system shall eventually satisfy burnout

Whenever burnout system shall at the next timepoint satisfy SeperationPhase

Whenever SeperationPhase system shall eventually satisfy transferorbit

REVIEW

Have you seen this pattern before?

Have you seen any variants of this pattern before?

Is it expressive enough? Is there anything missing from the pattern?

What system was this used for?

What sort of scenario or task was this used for?

Any general thoughts?

PATTERN 2: STAY-IN-PERIMETER

- Navigation for some autonomous space robotics is essential.
- Some systems need to maintain certain conditions while moving.
- During the movement/actions of some autonomous space robotics, robots are restricted to only moving/acting inside the perimeter.
- These safety restrictions are necessary for dynamic or uncontrolled environments for many moving systems

PATTERN STRUCTURE: STAY-IN-PERIMETER

- Let a be an action and c1, c2 be conditions

Whenever a system shall immediately satisfy c1 & c2

$$G(a \rightarrow (\bigwedge_{i=1}^{n} c_i))$$

EXAMPLES

- *"The SPHERES satellites, however, triangulate their position using infrared/ultrasonic beacons, preventing them from navigating outside the two-meter cube defined by the fixed beacon locations"*

  Whenever navigating SPHERES shall immediately satisfy x<2 & y<2 & z<2

- *"Int-Ball cannot operate without a direct line-of-sight to its markers."*

  Whenever operating IntBall2 shall immediately satisfy LOS1 & LOS2

REVIEW

Have you seen this pattern before?

Have you seen any variants of this pattern before?

Is it expressive enough? Is there anything missing from the pattern?

What system was this used for?

What sort of scenario or task was this used for?

Any general thoughts?

PATTERN 3: KEEP-OUT-ZONE

- Some systems need to avoid areas while operating
- During the movement/actions of some autonomous space robotics, robots are barred from entering specific areas

PATTERN STRUCTURE: KEEP-OUT-ZONE

- Let a be an action and c1, c2 be conditions

  Whenever a system shall immediately satisfy !c1 & !c2

$$G(a \rightarrow (\bigwedge_{i=1}^{n} \neg c_i))$$

EXAMPLE

- *"Astrobee's navigation and control systems understand the concept of a keep-out zone (KOZ). KOZs are defined as areas where Astrobee is not allowed to fly."*

Whenever moving Astrobee shall immediately satisfy !KOZ1 & !KOZ2

$$G(moving \rightarrow (\bigwedge_{i=1}^{n} \neg KOZ_i))$$

REVIEW

Have you seen this pattern before?

Have you seen any variants of this pattern before?

Is it expressive enough? Is there anything missing from the pattern?

What system was this used for?

What sort of scenario or task was this used for?

Any general thoughts?

PATTERN 4: TRANSMIT

- For the success of some systems, data needs to be transmitted
- But for data to be transmitted certain requirements need to be met
- Connection to the target and requested data need to be present

PATTERN STRUCTURE: TRANSMIT

- Let c represent the necessary connections, d the requested data and let T be the transmitting protocol.

  Whenever c & !d System shall until d satisfy T

$$G(((\bigwedge_{i=1}^{n} c_i) \wedge (\bigwedge_{i=1}^{n} \neg d_i)) \rightarrow (T \,\mathcal{U} \bigwedge_{i=1}^{n} d_i)))$$

EXAMPLE

- *“After a sortie, Astrobee transfers large files through a hard-wired Ethernet connection with its dock”*

  Whenever Ethernet & ISSConnection & !LargeFiles Astrobee shall until LargeFiles satisfy Transmit

- $G(((\text{Ethernet} \land \text{ISSConnection}) \land \neg\text{LargeFiles}) \rightarrow (\text{Transmit}\ U\ \text{LargeFiles}))$

REVIEW

Have you seen this pattern before?

Have you seen any variants of this pattern before?

Is it expressive enough? Is there anything missing from the pattern?

What system was this used for?

What sort of scenario or task was this used for?

Any general thoughts?

PATTERN 5: RECONNECT

- Connections are necessary for systems that need to communicate or transmit data.
- Connection can be disrupted in space applications, and it is essential to immediately restore that connection.
- This example focuses on systems that always attempt to re-establish a connection.

PATTERN STRUCTURE: RECONNECT

- Let c1 and c2 represent connections, R represents the reconnection protocol.

  Whenever !c1 | !c2 System shall until (c1 & c2) satisfy R

$$G\left(\left(\bigvee_{i=1}^{n} \neg c_i\right) \rightarrow \left(\mathrm{R}\; \mathcal{U} \bigwedge_{i=1}^{n} c_i\right)\right)$$

EXAMPLE

- The space-to-ground network is subject to frequent losses of signal. After loss-of-signal(LOS) astrobee shall attempt to reconnect.
- In this example both the connection to the ISS and the ISS connection to the ground control is lost

Whenever !GroundSignal | !ISSConnection Astrobee shall until (ISSConnection & GroundSignal) satisfy Reconnect

- G (((! GroundSignal) | (! ISSConnection)) -> (Reconnect U (ISSConnection & GroundSignal)))

REVIEW

Have you seen this pattern before?

Have you seen any variants of this pattern before?

Is it expressive enough? Is there anything missing from the pattern?

What system was this used for?

What sort of scenario or task was this used for?

Any general thoughts?

Any last thoughts?