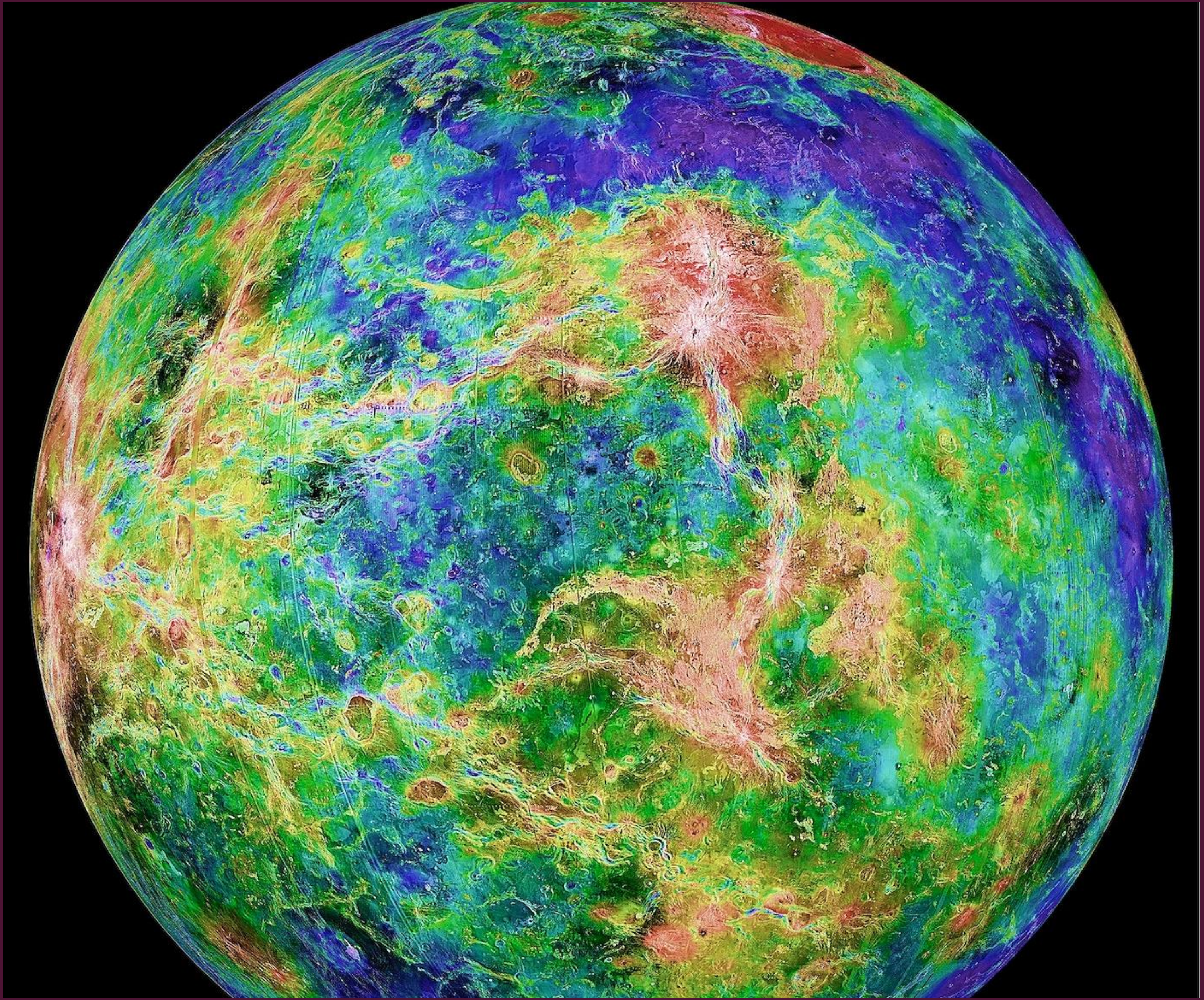
SAFELY NAVIGATING THE SURFACE OF VENUS: MODEL CHECKING A MECHANICAL OBSTACLE AVOIDANCE SENSOR IN NUXMV

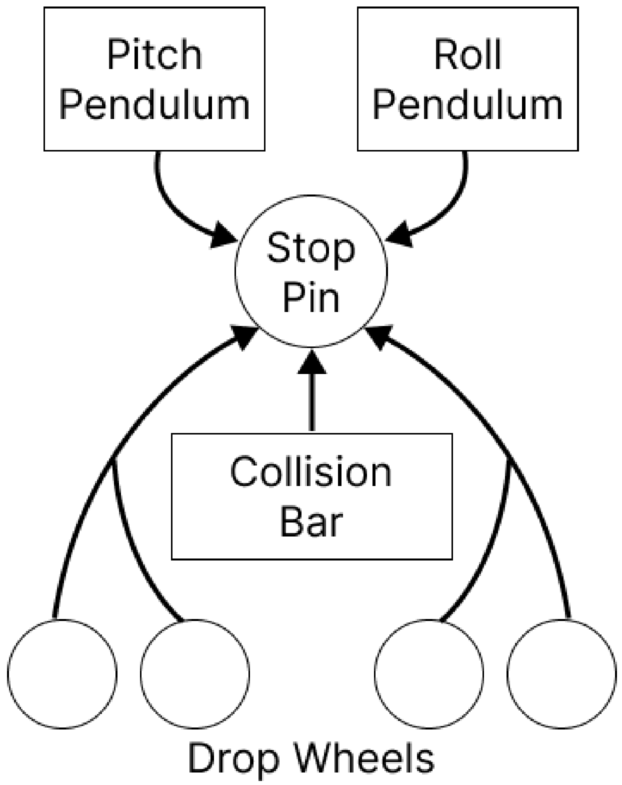
ELIZABETH SLOAN, ERIN ASHLEY

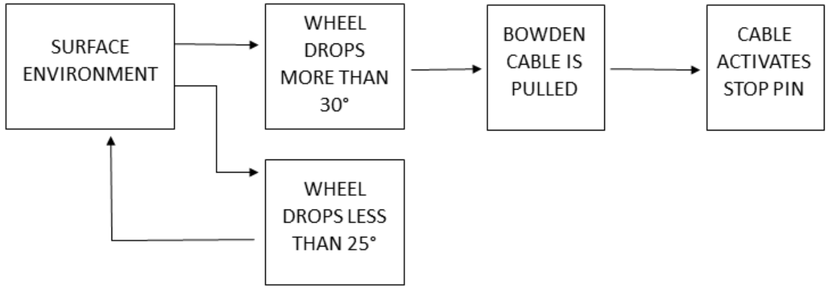


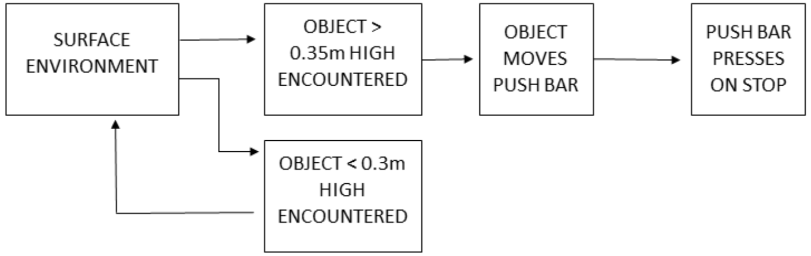
HOW DO WE NAVIGATE THE SURFACE OF HELL?

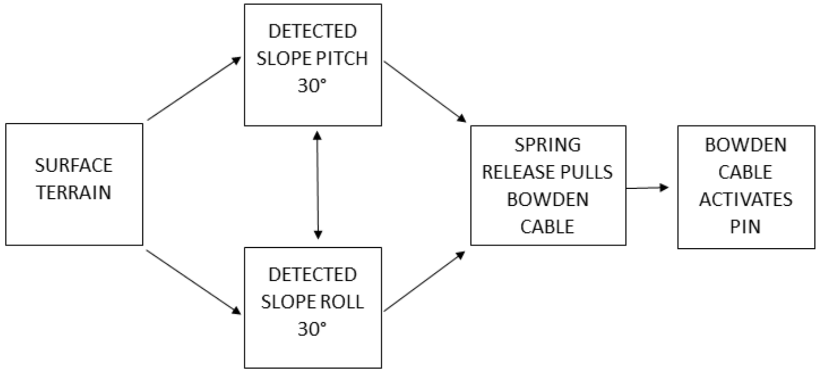
Avoid	Steep slopes and inclines
Avoid	Large rocks and other obstacles
Avoid	Holes and cliffs

A CLOCKWORK ROVER – SYSTEM AND ABSTRACTIONS



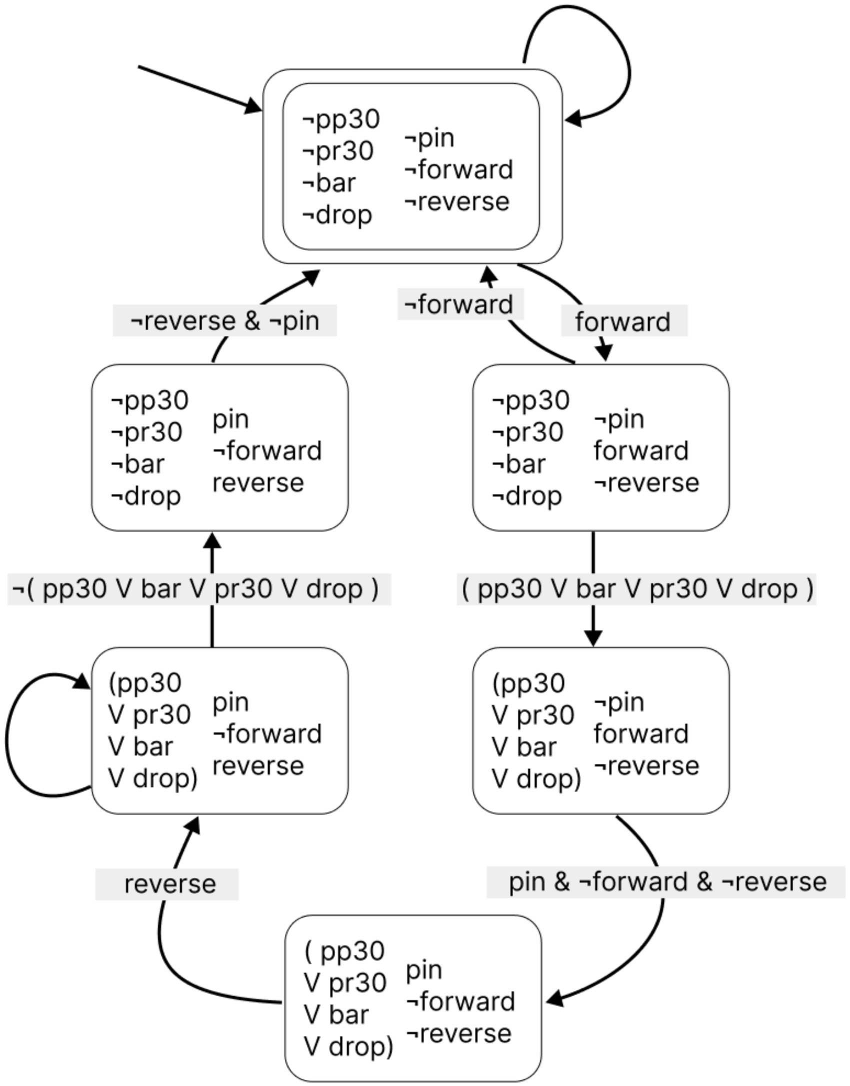




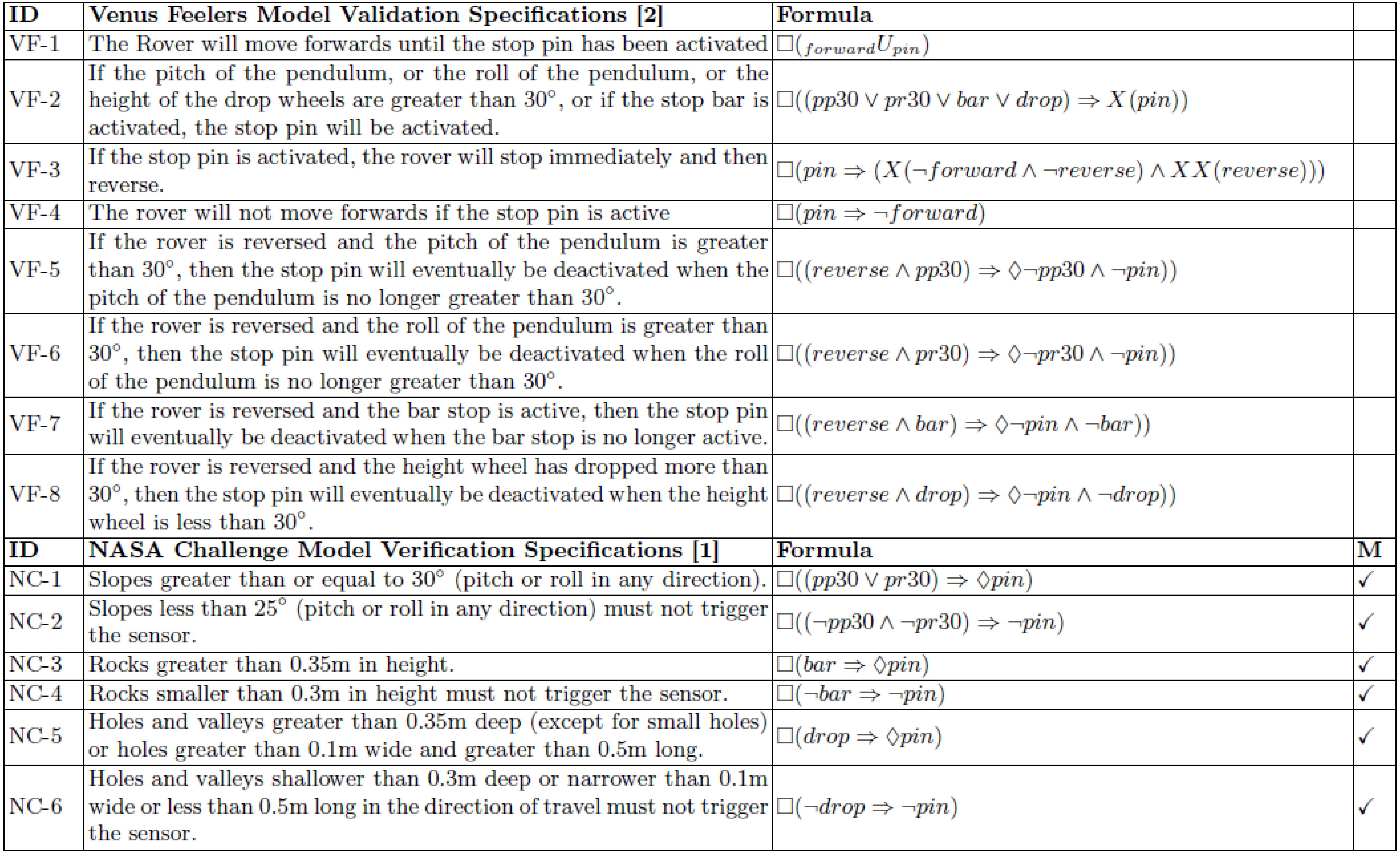


REDUCING THE STATE SPACE

- Each module can be abstracted as a **1 or 2 variables**
- System input variables are **independent** of each other
- State space reduces from 62 to 6



TRANSLATING ENGLISH TO LTL



ID	Venus Feelers Model Validation Specifications [2]	Formula	
VF-1	The Rover will move forwards until the stop pin has been activated	$\Box(_{forward}U_{pin})$	
VF-2	If the pitch of the pendulum, or the roll of the pendulum, or the height of the drop wheels are greater than 30°, or if the stop bar is activated, the stop pin will be activated.	$\Box((pp30 \vee pr30 \vee bar \vee drop) \Rightarrow X(pin))$	
VF-3	If the stop pin is activated, the rover will stop immediately and then reverse.	$\Box(pin \Rightarrow (X(\neg forward \wedge \neg reverse) \wedge XX(reverse)))$	
VF-4	The rover will not move forwards if the stop pin is active	$\Box(pin \Rightarrow \neg forward)$	
VF-5	If the rover is reversed and the pitch of the pendulum is greater than 30°, then the stop pin will eventually be deactivated when the pitch of the pendulum is no longer greater than 30°.	$\Box((reverse \wedge pp30) \Rightarrow \Diamond\neg pp30 \wedge \neg pin))$	
VF-6	If the rover is reversed and the roll of the pendulum is greater than 30°, then the stop pin will eventually be deactivated when the roll of the pendulum is no longer greater than 30°.	$\Box((reverse \wedge pr30) \Rightarrow \Diamond\neg pr30 \wedge \neg pin))$	
VF-7	If the rover is reversed and the bar stop is active, then the stop pin will eventually be deactivated when the bar stop is no longer active.	$\Box((reverse \wedge bar) \Rightarrow \Diamond\neg pin \wedge \neg bar))$	
VF-8	If the rover is reversed and the height wheel has dropped more than 30°, then the stop pin will eventually be deactivated when the height wheel is less than 30°.	$\Box((reverse \wedge drop) \Rightarrow \Diamond\neg pin \wedge \neg drop))$	
ID	**NASA Challenge Model Verification Specifications [1]**	**Formula**	**M**
NC-1	Slopes greater than or equal to 30° (pitch or roll in any direction).	$\Box((pp30 \vee pr30) \Rightarrow \Diamond pin)$	✓
NC-2	Slopes less than 25° (pitch or roll in any direction) must not trigger the sensor.	$\Box((\neg pp30 \wedge \neg pr30) \Rightarrow \neg pin)$	✓
NC-3	Rocks greater than 0.35m in height.	$\Box(bar \Rightarrow \Diamond pin)$	✓
NC-4	Rocks smaller than 0.3m in height must not trigger the sensor.	$\Box(\neg bar \Rightarrow \neg pin)$	✓
NC-5	Holes and valleys greater than 0.35m deep (except for small holes) or holes greater than 0.1m wide and greater than 0.5m long.	$\Box(drop \Rightarrow \Diamond pin)$	✓
NC-6	Holes and valleys shallower than 0.3m deep or narrower than 0.1m wide or less than 0.5m long in the direction of travel must not trigger the sensor.	$\Box(\neg drop \Rightarrow \neg pin)$	✓

BUT WAIT – HOW DO WE KNOW OUR MODEL IS CORRECT?

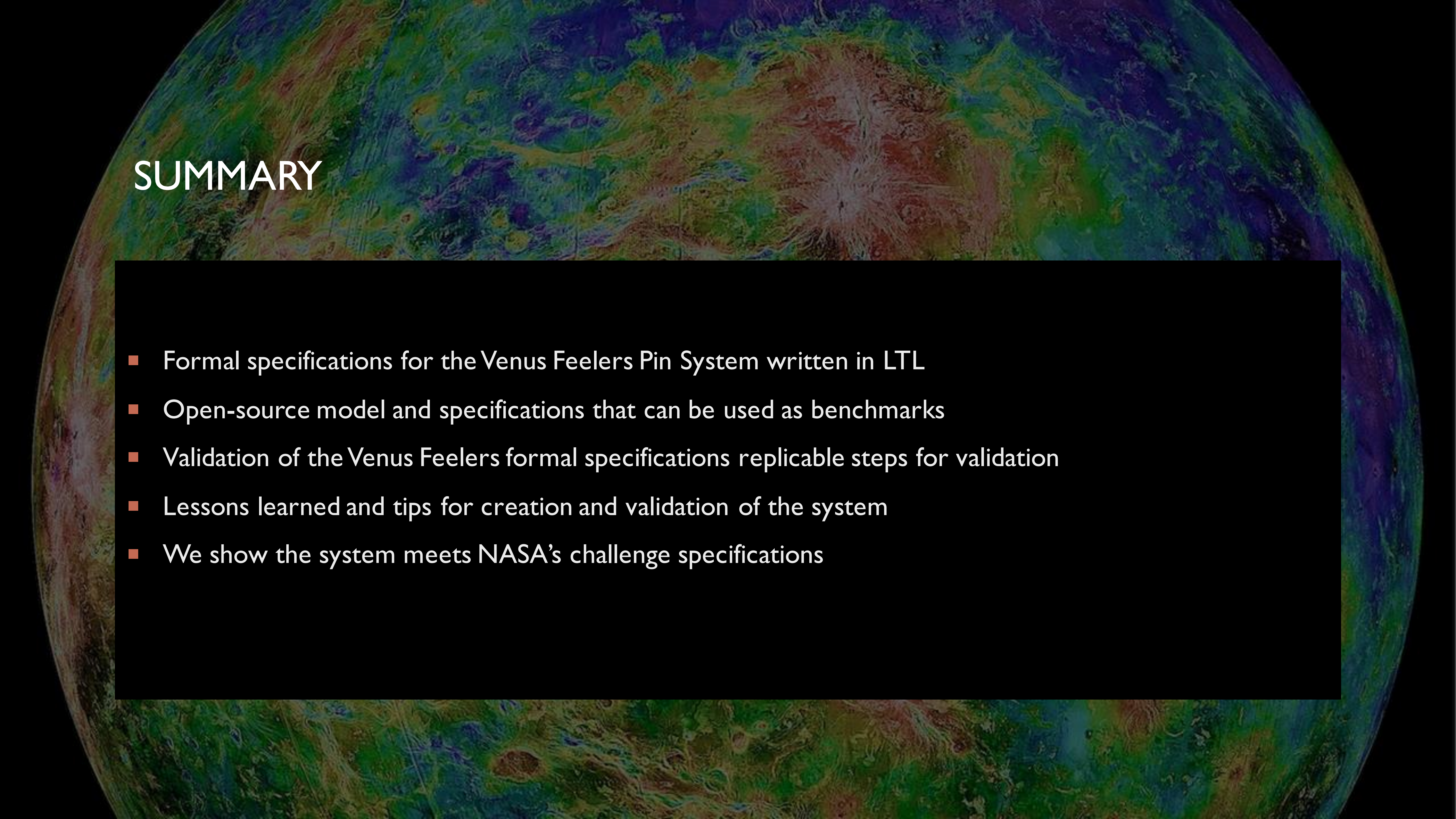
- Checking our model against the validation specifications
- **No discrepancies** were found
- Disclaimer: **only** for the physical portion of the system

VERIFICATION RESULTS

- Counterexample traces returned for **all** negations of LTL properties!
- System vacuously true if the rover **never moves**
- System vacuously true if the rover **reverses forever**
- No detection system **behind** the rover
- No system to allow the rover to **change direction**

FUTURE WORK

- Review LTL verification specifications with JPL engineers
- Expand formal specifications for future cyber system component
- Continually update model as development continues
- Make sure future bugs addressed
- Use this study for project-based learning



SUMMARY

- Formal specifications for the Venus Feelers Pin System written in LTL
- Open-source model and specifications that can be used as benchmarks
- Validation of the Venus Feelers formal specifications replicable steps for validation
- Lessons learned and tips for creation and validation of the system
- We show the system meets NASA’s challenge specifications