SAPIENZA
UNIVERSITÀ DI ROMA

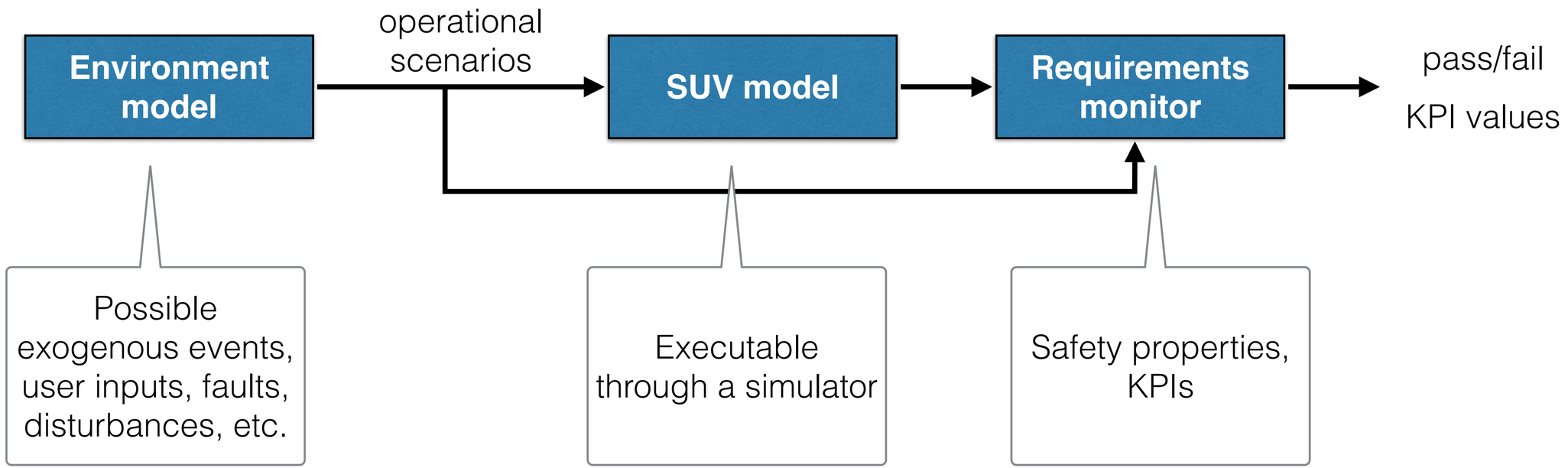
MClab

Automatic Generation of Simulation Scenarios for Statistical Model Checking of Real-Time Systems [*]

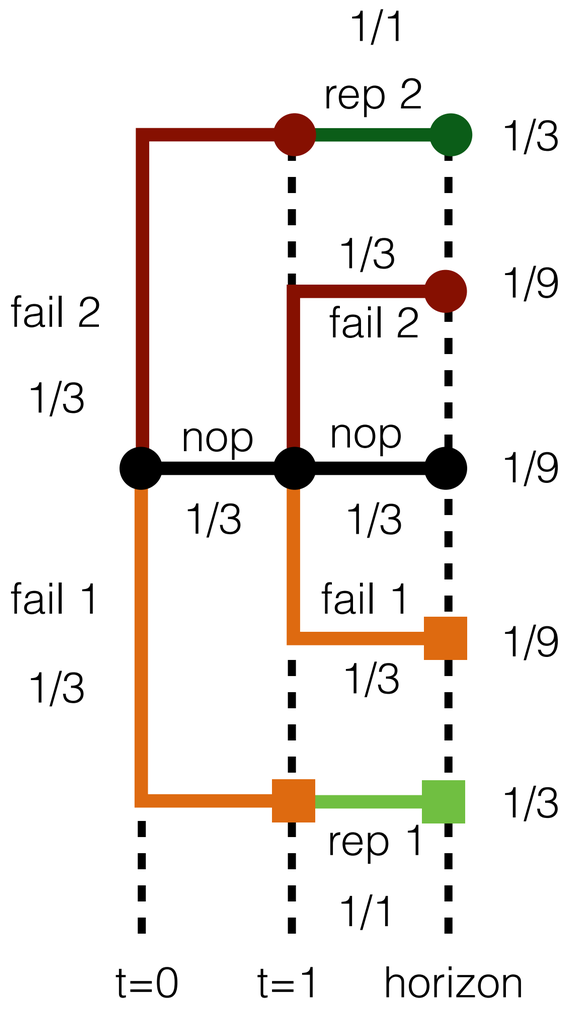
Toni Mancini, Igor Melatti, *Enrico Tronci*
Department of Computer Science
Sapienza University of Rome, Italy
mclab.di.uniroma1.it

[*] Toni Mancini, Igor Melatti, Enrico Tronci.
Any-horizon Uniform Random Sampling and Enumeration of Constrained Scenarios for Simulation-based Formal Verification.
IEEE Transactions on Software Engineering, 2021. DOI: 10.1109/TSE.2021.3109842

Simulation-based verification



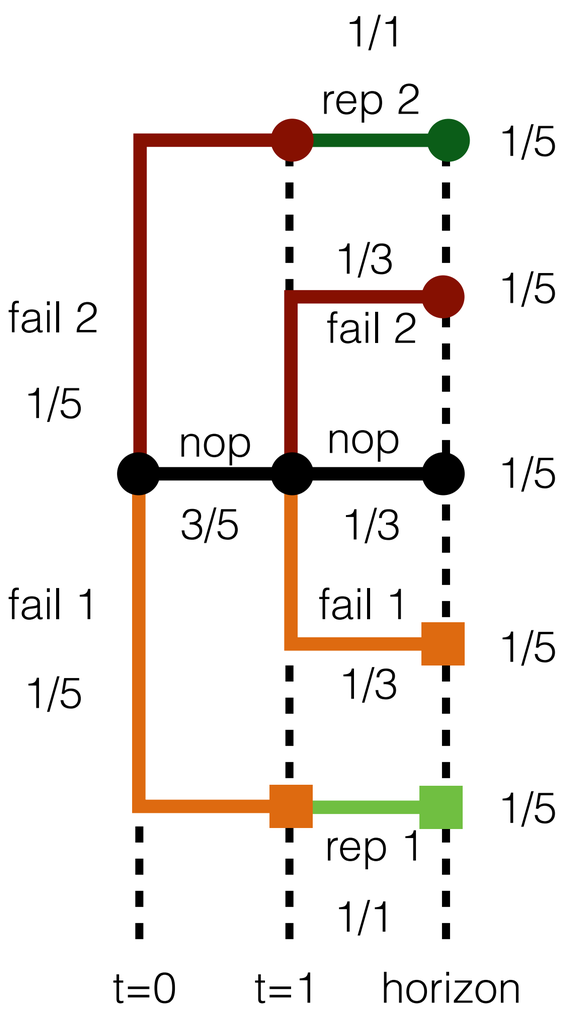
Sampling events vs. sampling scenarios



Uniform sampling of scenarios yields minimum worst-case expected verification time [1].
Not easy to obtain.

Uniform sampling of admissible events **does not** yield a uniform sampling of admissible scenarios

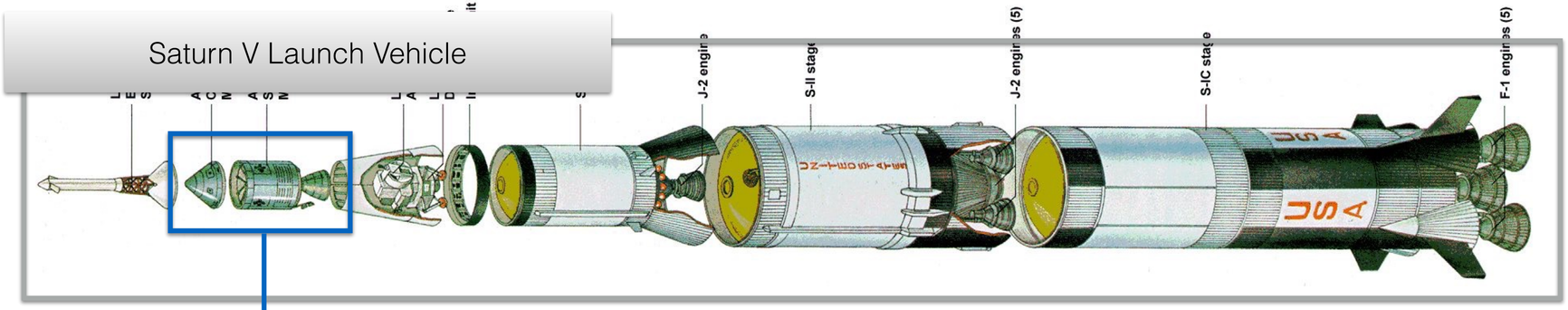
Uniform sampling of scenarios requires **suitable probabilities** for occurrences of events **at each node**

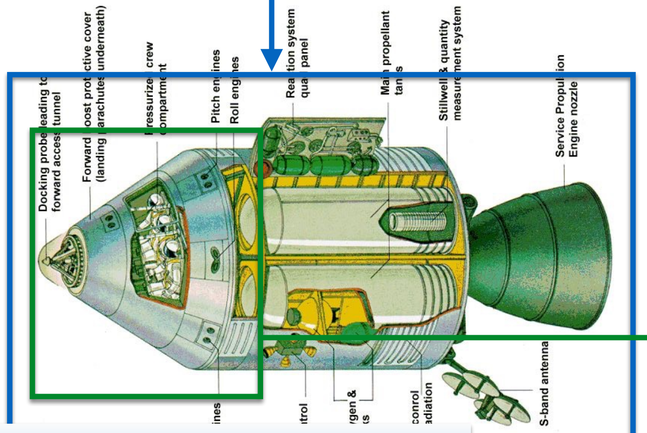


[1] T. Mancini, et al. *On minimising the maximum expected verification time.* Information Processing Letters 122, 2017

Example: Apollo Lunar Module Autopilot (ALMA)

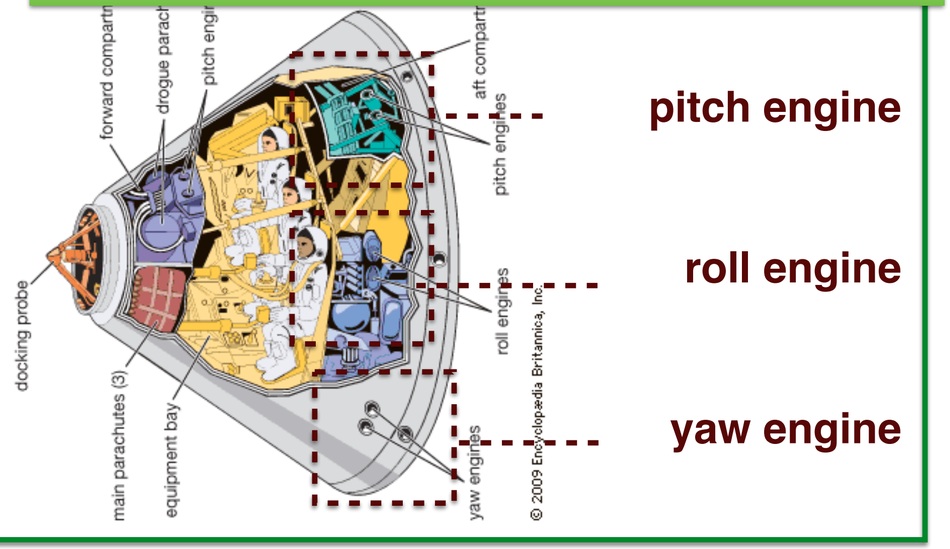
Saturn V Launch Vehicle





Apollo Command and Service Modules

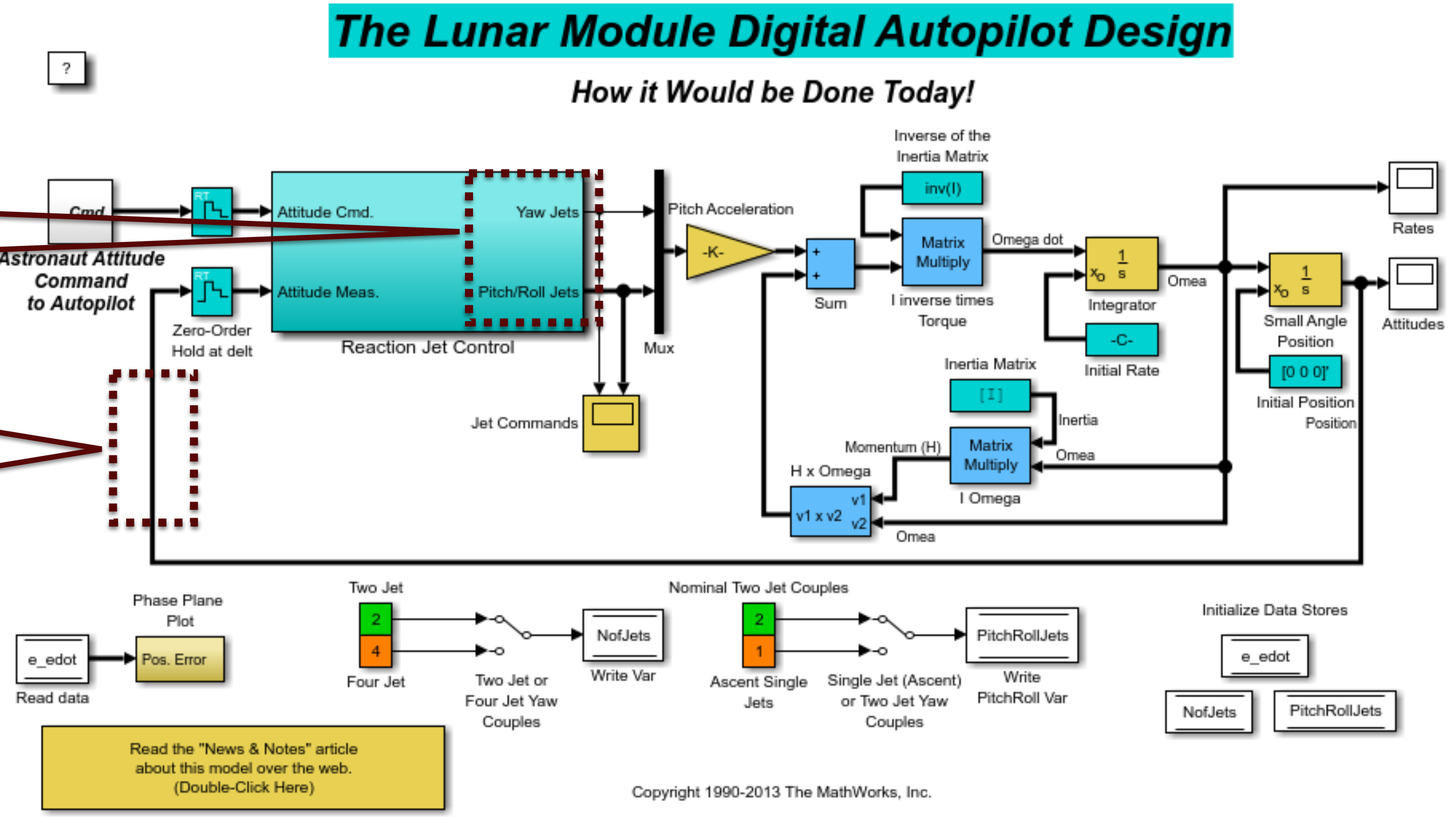
Apollo Command Module



Example: ALMA Simulink model

16 reaction jets (actuators)

Three signals: Yaw, Pitch and Roll sensors



Safety: Yaw, Pitch and Roll close to 0

MATLAB SIMULINK

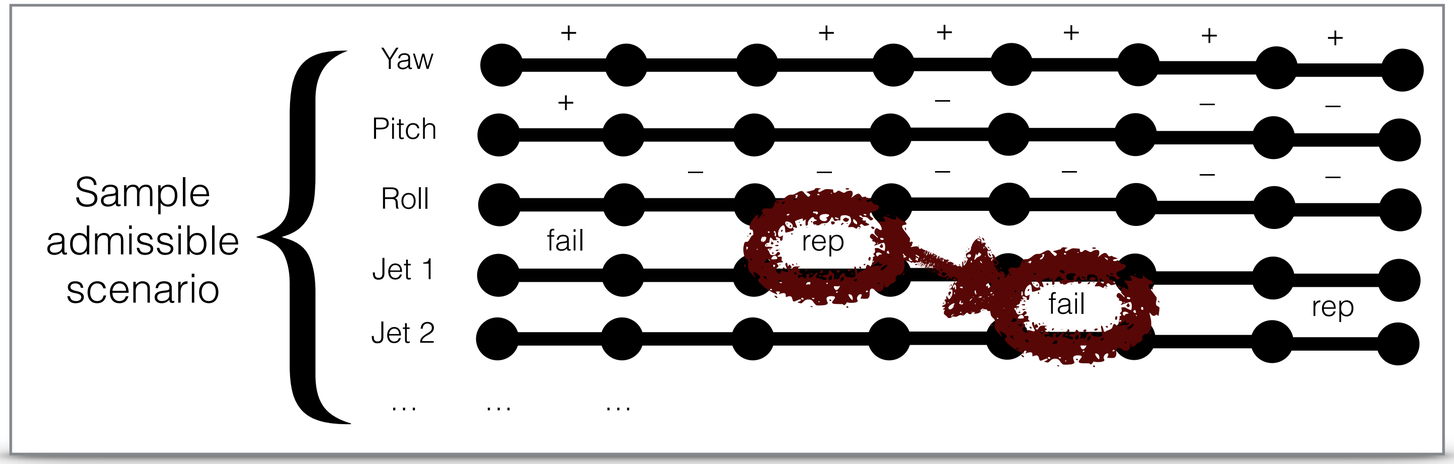
SUV environment: ALMA

Events

- **Inputs from autopilot:**
  - Time series of module attitude change requests (Yaw, Pitch, Roll)
- **Faults and disturbances**
  - Additive errors on attitude sensors (current orientation: Yaw, Pitch, Roll)
  - Temporary faults on reaction jets (actuators)

Requirements

- **Assumptions**
  - No immediate undo of attitude change requests
  - Noise signals chosen from portfolio and changing during time
  - Jets recovery from faults with 2-3 time units
- **Additional requirements to focus verification**
  - No multiple jets faulty at the same time



Our approach [1]

1. **Requirements on environment events via composable finite states machines (monitors)**
   - Defined through user-friendly Python- or Modelica-based languages
2. **Scenario generators automatically computed, offering API to return:**
   - number of admissible scenarios of given length h (horizon)
   - the i-th lex-ordered admissible scenario of length h

The above seamlessly supports all sorts of verification activities:

- statistical model checking (via **uniform** random sampling of admissible scenarios)
- exhaustive (possibly **uniformly randomised**) verification, **minimising worst-case expected verification time** [2]

[1] T. Mancini *et al*. *Any-horizon Uniform Random Sampling and Enumeration of Constrained Scenarios for Simulation-based Formal Verification.* IEEE Transactions on Software Engineering, 2021. DOI: 10.1109/TSE.2021.3109842

[2] T. Mancini, et al. *On minimising the maximum expected verification time.* Information Processing Letters 122, 2017

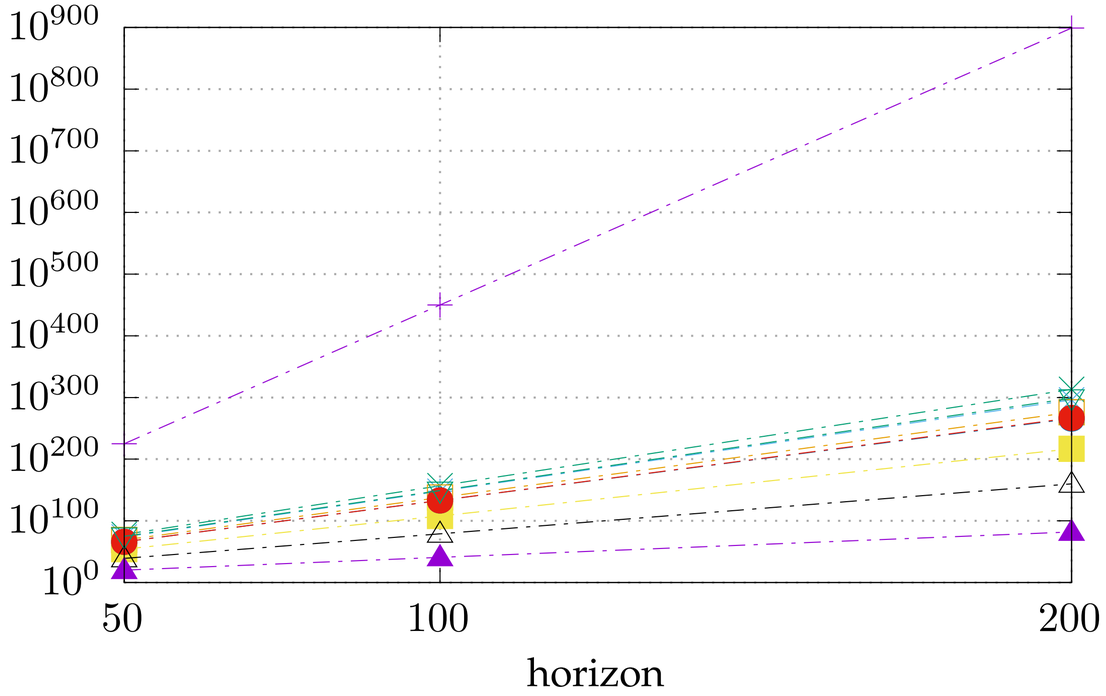
Experimental results: computation of scenario generators

SUV	SG nb.	$\mathcal{M}$			$Gen(\mathcal{M})$
		assumptions monitor	constraint monitors	size of input space	time [s]
Apollo Lunar Module Autopilot	1	$\mathcal{A}_{\text{rj}}$	–	1 769 472	0.44
	2	$\mathcal{A}_{\text{rj}}$	1	108	0.44
	3	$\mathcal{A}_{\text{rj}}$	1, 2	108	448.88
	4	$\mathcal{A}_{\text{rj}}$	1, 2, 3	108	247.27
	5	$\mathcal{A}_{\text{rj}}$	1, 2, 3, 4	108	55.19
	6	$\mathcal{A}_{\text{rj}}$	1, 2, 3, 5	108	188.3
	7	$\mathcal{A}_{\text{s}}$	–	27	2.94
	8	$\mathcal{A}_{\text{s}}$	6	27	1.33
	9	$\mathcal{A}_{\text{s}}$	6, 7	27	782.2
	10	$\mathcal{A}_{\text{ALMA}}$	1, 2, 3, 4, 6, 7	2916	837.39

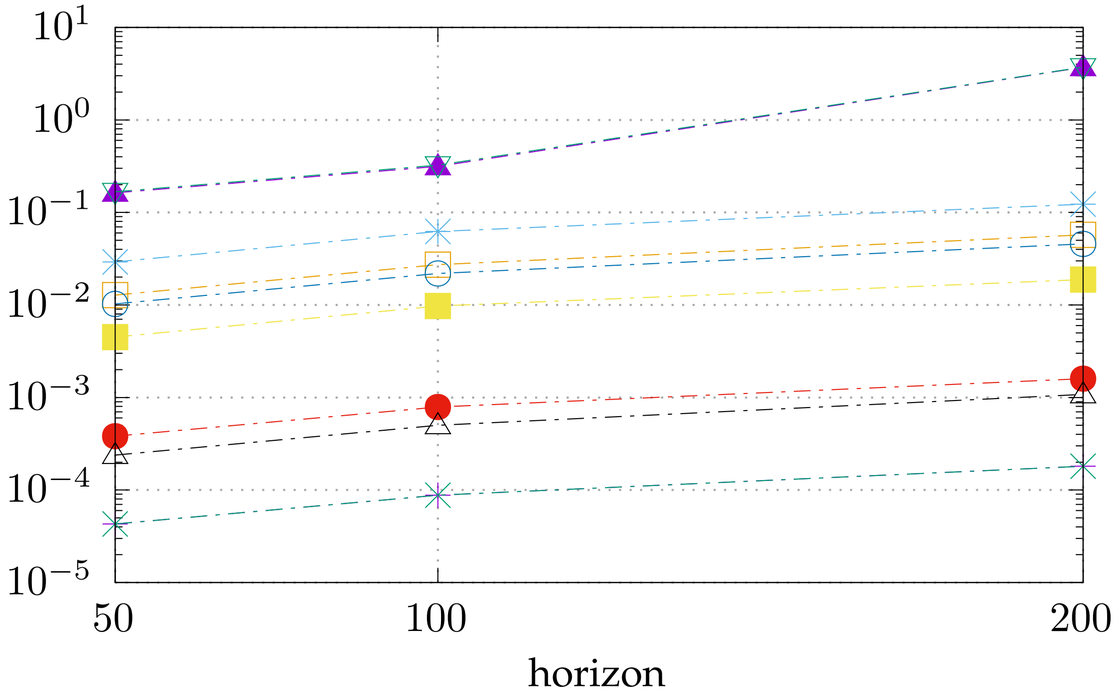
SUV	SG nb.	$\mathcal{M}$			$Gen(\mathcal{M})$
		assumptions monitor	constraint monitors	size of input space	time [s]
Buck DC/DC Converter	1	$\mathcal{A}_i$	–	5	0.19
	2	$\mathcal{A}_R$	–	5	0.17
	3	$\mathcal{A}_i \bowtie \mathcal{A}_R$	–	25	0.36
	4	$\mathcal{A}_i$	1	5	0.12
	5	$\mathcal{A}_i$	2	5	0.17
	6	$\mathcal{A}_R$	3	5	0.11
	7	$\mathcal{A}_R$	4	5	0.16
	8	$\mathcal{A}_i \bowtie \mathcal{A}_R$	5	25	37.34
	9	$\mathcal{A}_i \bowtie \mathcal{A}_R$	2, 4, 5	25	29.68
	10	$\mathcal{A}_i \bowtie \mathcal{A}_R$	2, 4, 5, 6	25	1.94
	11	$\mathcal{A}_i \bowtie \mathcal{A}_R$	1, 3, 5, 7	25	2.16

SUV	SG nb.	$\mathcal{M}$			$Gen(\mathcal{M})$
		assumptions monitor	constraint monitors	size of input space	time [s]
Fault-Tolerant Fuel Control System	1	$\mathcal{A}_{\text{FCS}}$	–	6	0.1
	2	$\mathcal{A}_{\text{FCS}}$	1	6	7.99
	3	$\mathcal{A}_{\text{FCS}}$	1, 3	6	4.92
	4	$\mathcal{A}_{\text{FCS}}$	1, 2	6	4.61
	5	$\mathcal{A}_{\text{FCS}}$	1, 4	6	6.34
	6	$\mathcal{A}_{\text{FCS}}$	1, 4, 5	6	5.92
	7	$\mathcal{A}_{\text{FCS}}$	1, 4, 6	6	6.55

Experimental results: scenario extraction



Number of traces



Trace extraction time [s]

Apollo Lunar Module Autopilot

SAPIENZA
UNIVERSITÀ DI ROMA

MCLab

Thank you

Automatic Generation of Simulation Scenarios for Statistical Model Checking of Real-Time Systems [*]

Toni Mancini, Igor Melatti, Enrico Tronci
Department of Computer Science | Sapienza University of Rome, Italy | mclab.di.uniroma1.it

[*] Toni Mancini, Igor Melatti, Enrico Tronci. Any-horizon Uniform Random Sampling and Enumeration of Constrained Scenarios for Simulation-based Formal Verification. IEEE Transactions on Software Engineering, 2021. DOI: 10.1109/TSE.2021.3109842