Safety MOnitoring Framework (SMOF)

Lola Masson, Mathilde Machin,
Jérémie Guiochet, Hélène Waeselynck,
Matthieu Roy

https://www.laas.fr/projects/smof/

Introduction

LAAS-CNRS (Laboratoire d'Analyse et d'Architecture des Systèmes) in Toulouse

Team TSF (Tolérance aux Fautes et Sûreté de Fonctionnement informatique)

-> fault prevention
-> fault tolerance
-> fault elimination
-> fault evaluation

Dependable robots @laas

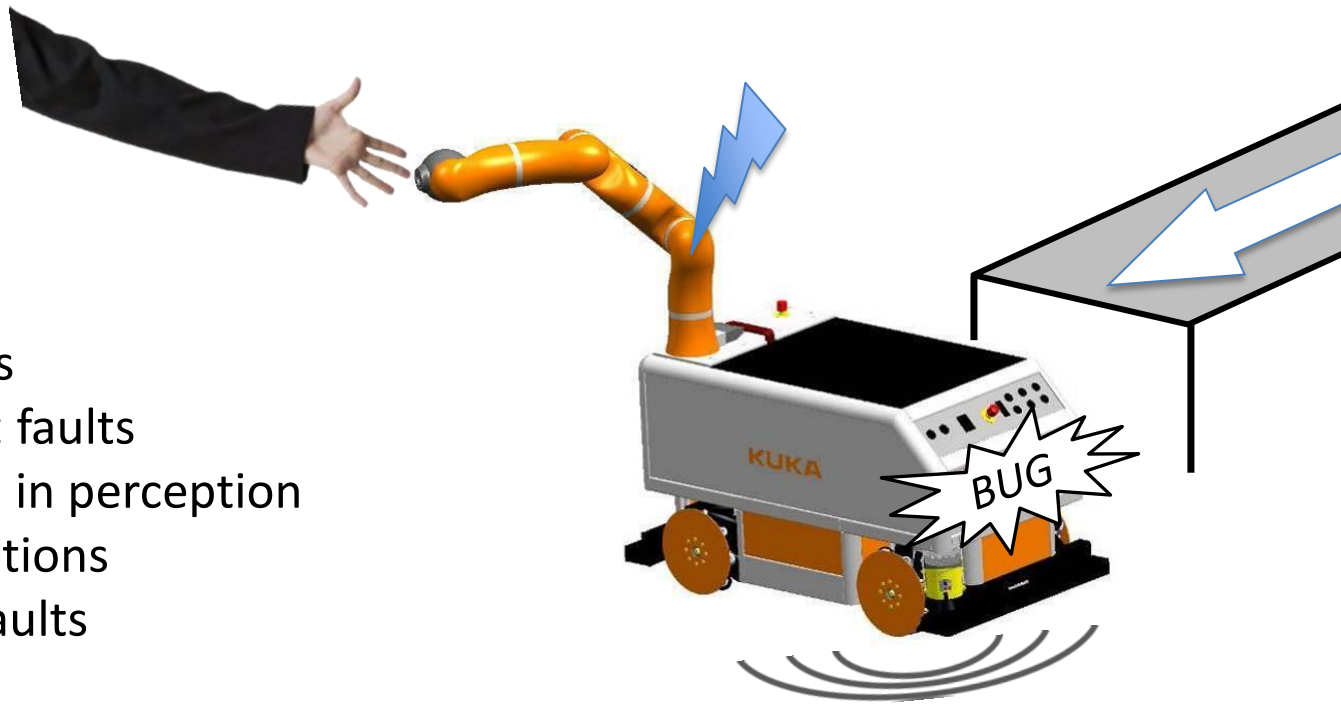
- Phds :
  - Execution Monitoring (2005) , Diverse task planning (2007), Robustness testing (2011), Safety monitoring (2012), Safety analysis for human-robot interactions (2015), Safety monitoring (with synthesis) (2015), Testing autonomous robots in virtual worlds, Multi-level safety monitoring

- Recent collaborative European projects :
  - **CPS Engineering Labs**: cyber physical systems, European H2020-ICT, 2015-2018
  - **SAPHARI** : Safe and Autonomous Physical Human-Aware Robot Interaction, FP7 European Project, 2011-2014
  - **PHRIENDS**: Physical Human-Robot Interaction: depENDability and Safety, FP6 European project, 2006-2009

Our Focus: Safe Autonomous robots

Cyber-physical systems + mobility + decisional capabilities

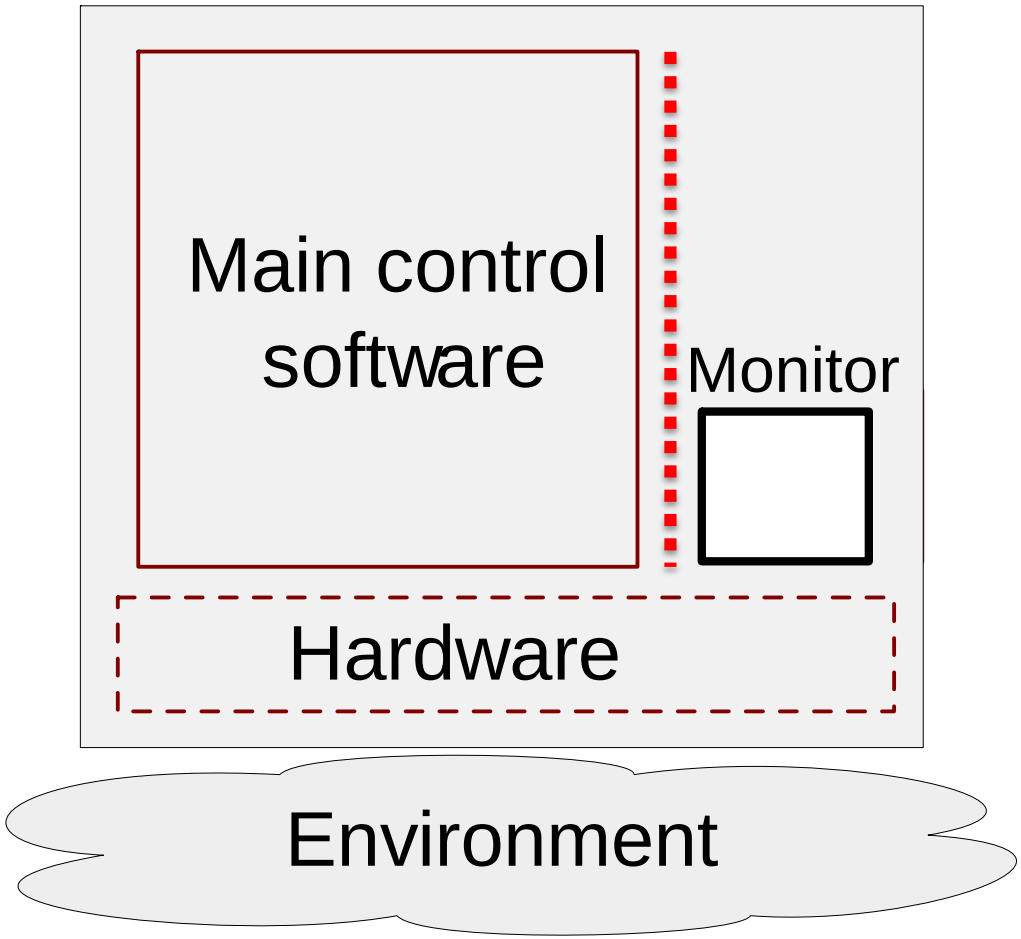
E.g.: ground robots, intelligent cars, UAVs



Threats:

- Physical faults
- Development faults
- Uncertainties in perception
- Adverse situations
- Interaction Faults

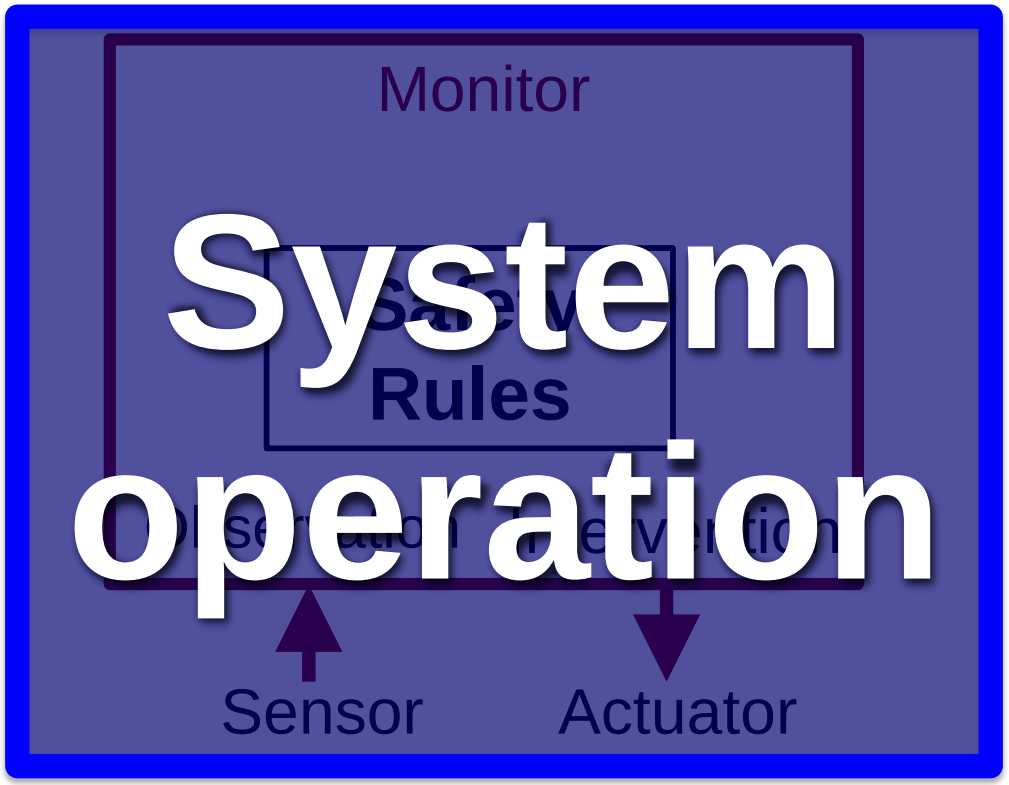
Safety Monitor



Safety Rules

Properties required from the monitor:

- Safety
- Permissiveness

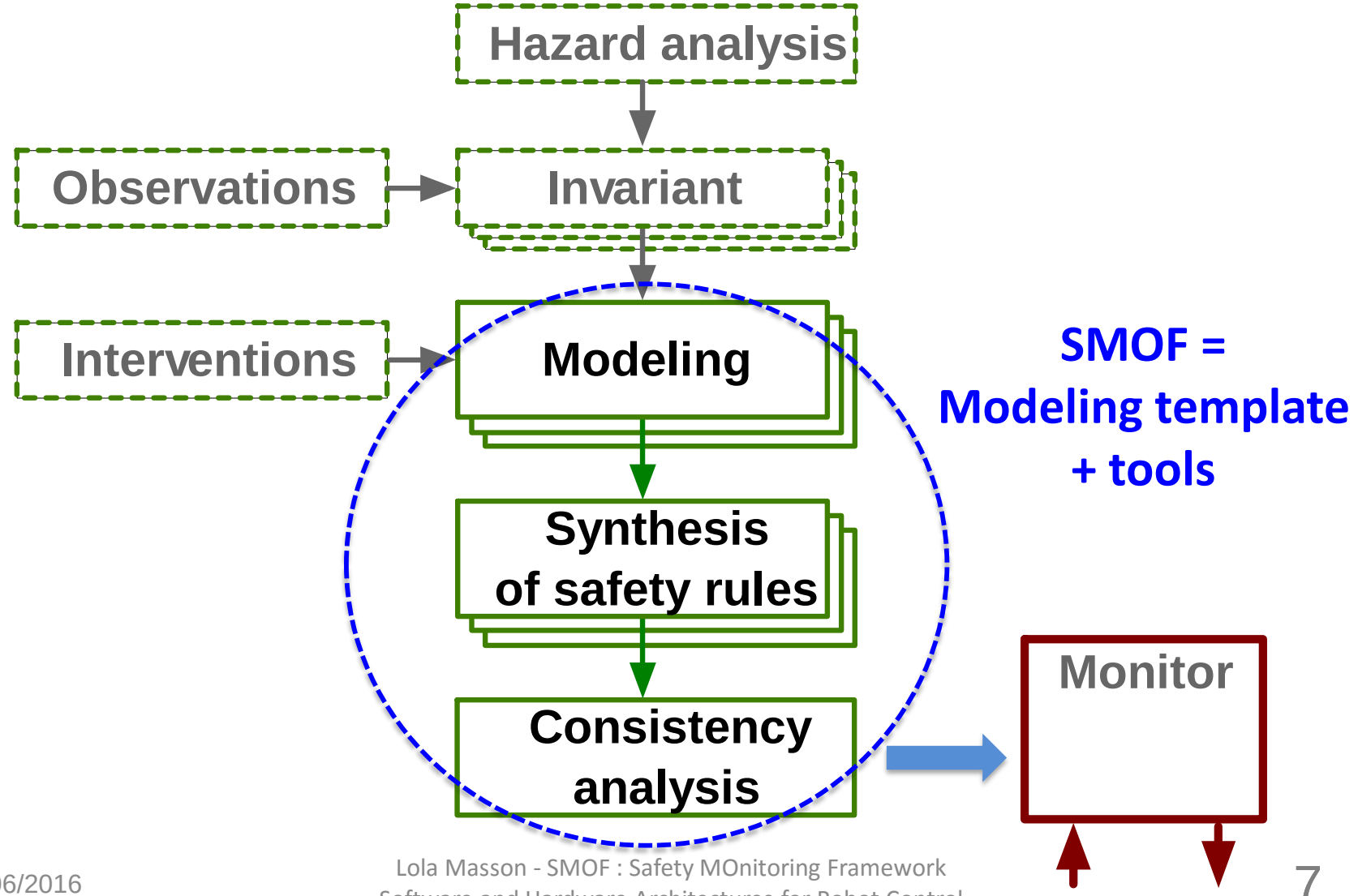


System operation

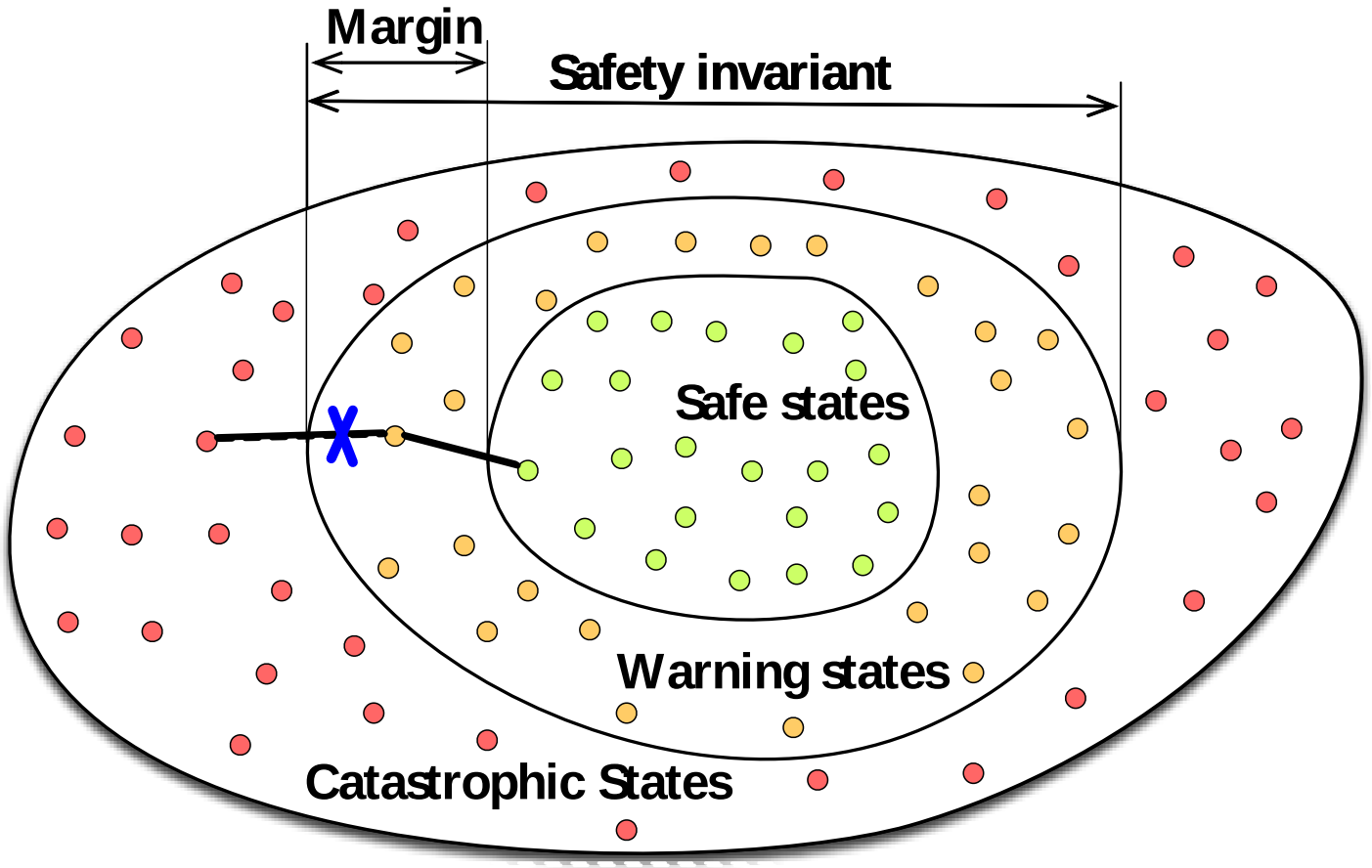
System design

⇒ Specification of the safety rules

Method overview



Concepts: margin, warning states

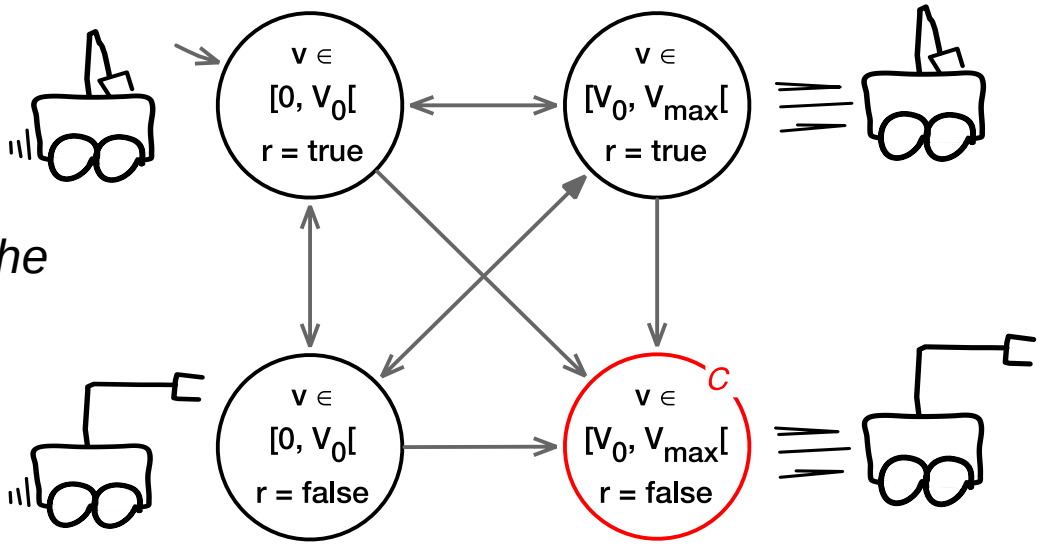


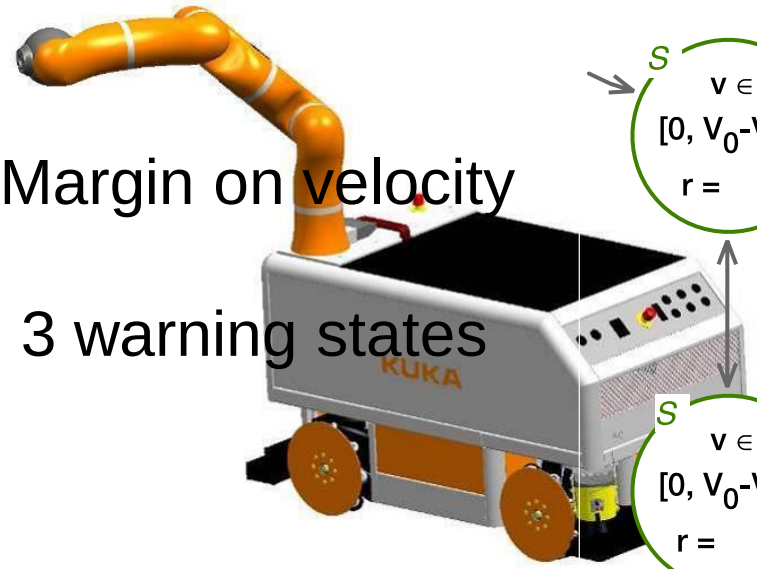
- A safety rule assigns interventions to warning states
- A **strategy** is a set of safety rules intended to ensure an invariant

Illustration on an example

The robot arm must be folded when the platform velocity is greater than V_0

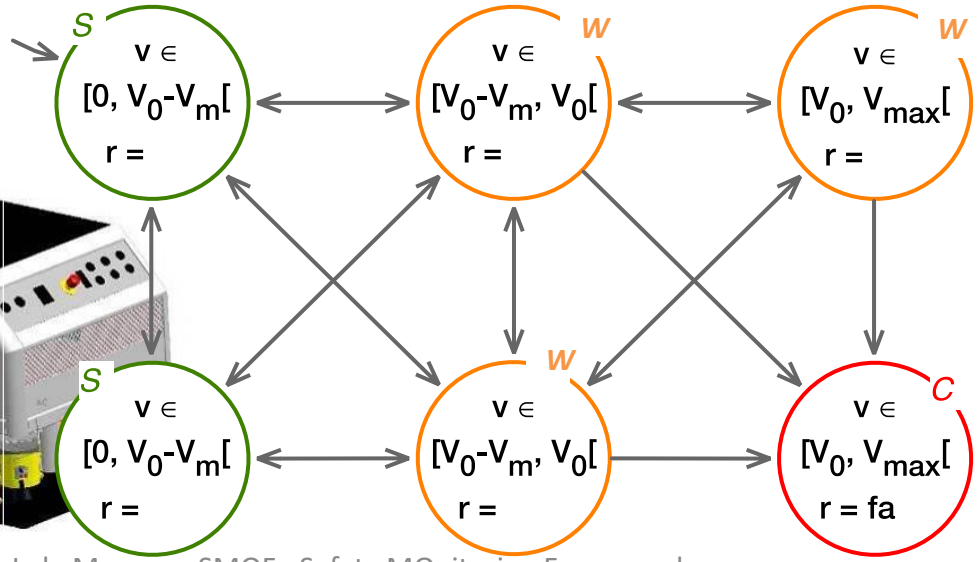
$(a = \text{true}) \vee (v < V_0)$





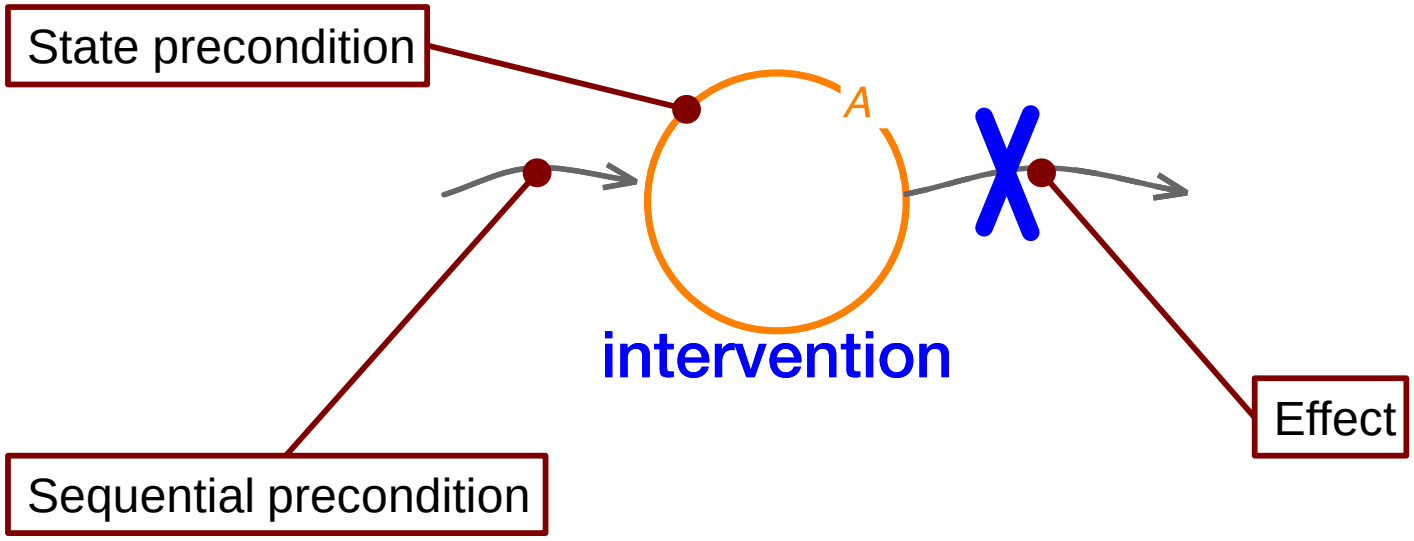
Margin on velocity

3 warning states



Interventions

- Ability of the monitor to constrain the system behavior
- E.g.: engage platform brakes, lock the arm position
- Effect under preconditions



Modeling with SMOF

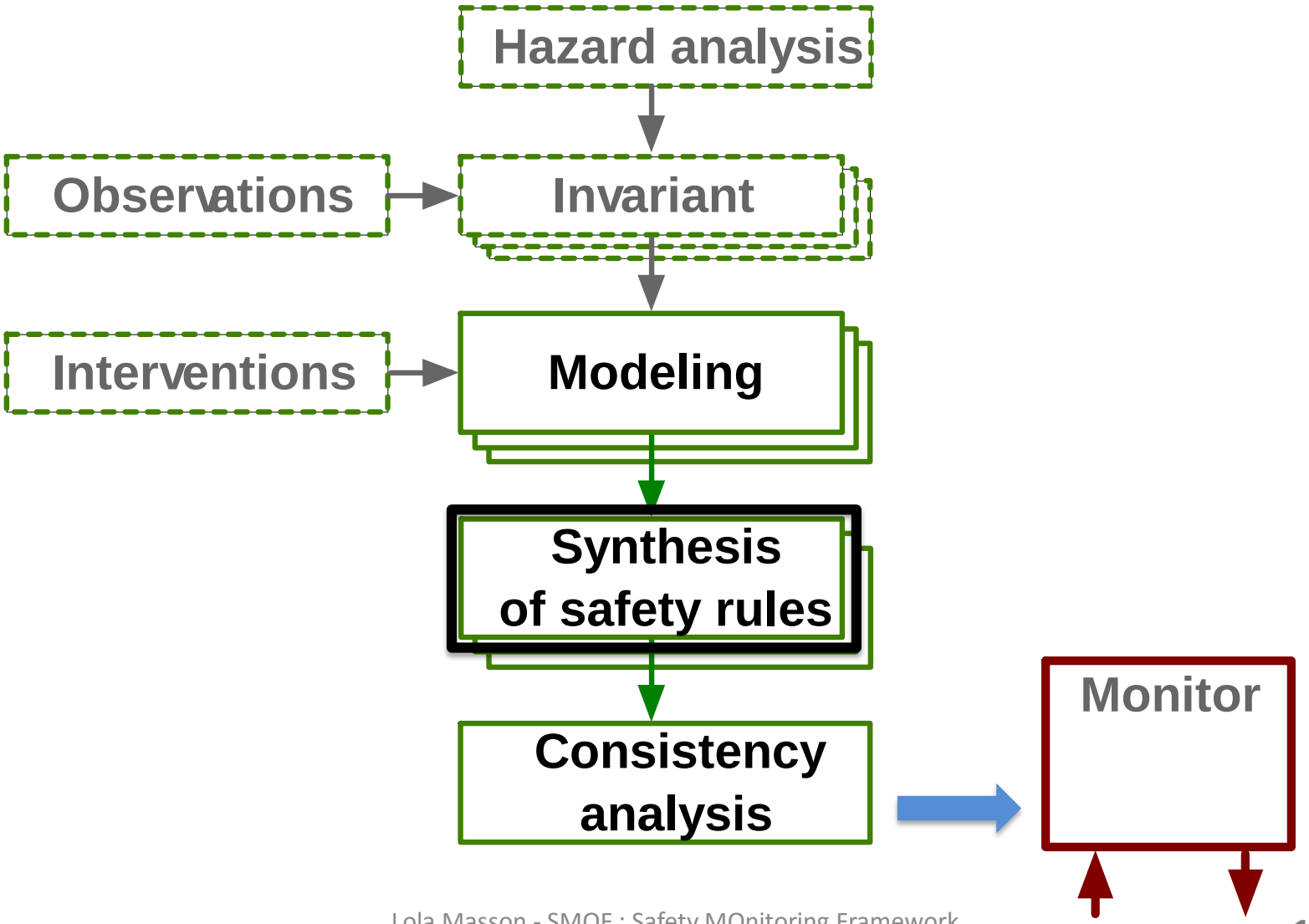
- NuSMV
- SMOF template:
  - Predefined parts
  - Parts to be edited by the user
  - Generated parts

```
VAR
pf_vel: Continuity(0,2,0);
arm_pos : Continuity(0,1,1);

DEFINE cata:= (pf_vel=2 & arm_pos=0);

VAR
brake : Intervention(TRUE, pf_vel!=0, flag_brake, next(pf_vel)=pf_vel!=2);
lock_arm : Intervention(arm_pos=1, TRUE, flag_lock_arm, next(arm_pos)=1);
```

Method


Hazard analysis
Observations
Invariant
Interventions
Modeling
Synthesis of safety rules
Consistency analysis
Monitor

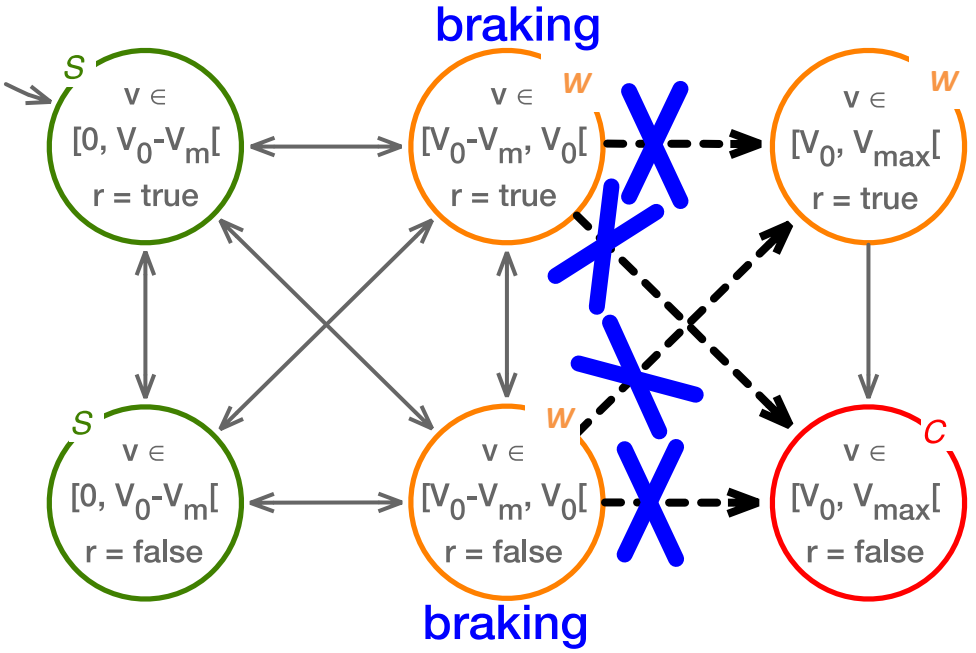
Strategies

- Association

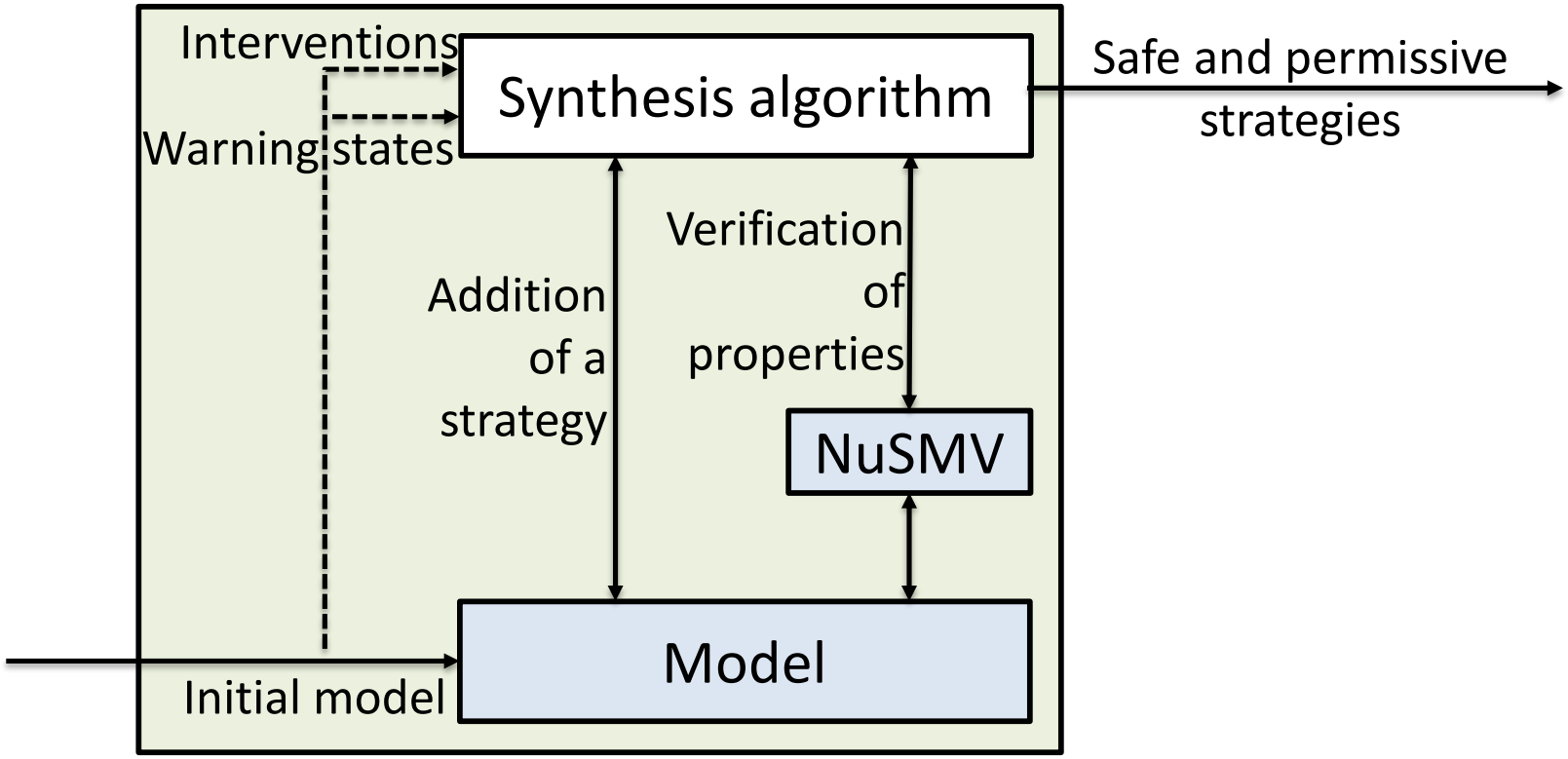
  Warning state – combination of interventions

- Required properties:
  - **Safe**: catastrophic states are not reachable
  - **Permissive**: non-catastrophic states are reachable

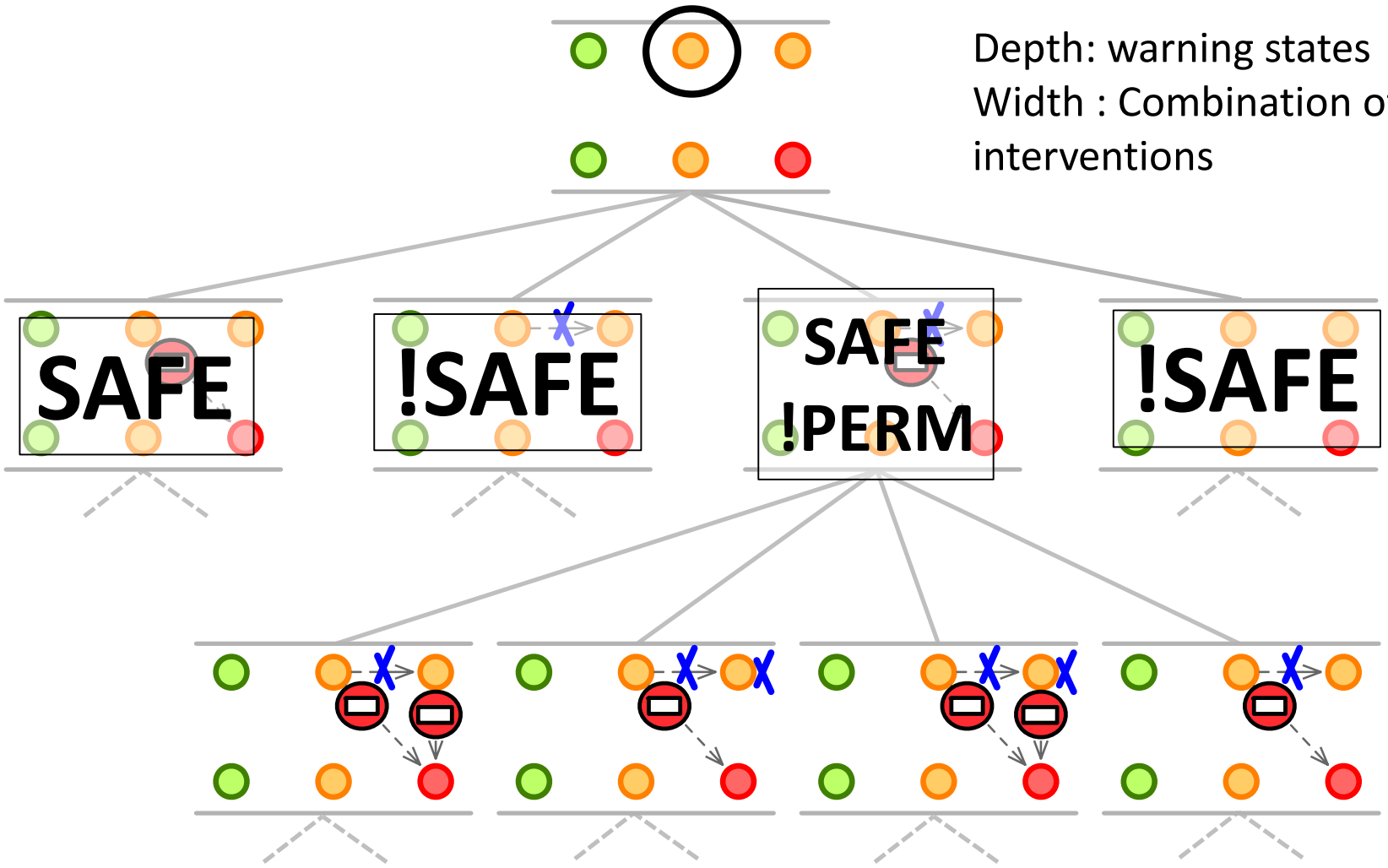
This strategy is safe,
but not permissive !



Synthesis of strategies

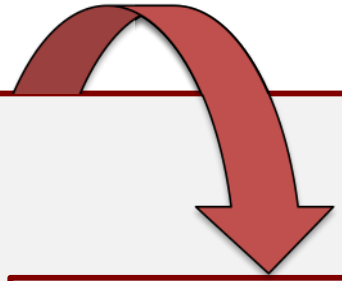


Tree of strategies



Depth: warning states
Width : Combination of interventions

Exemplary result



```
VAR
pf_vel: Continuity(0,2,0);
arm_pos : Continuity(0,1,1);

DEFINE cata:= (pf_vel=2 & arm_pos=0)
--Safety property
INVARSPEC !cata

-- Intervention(precondition, flag,
VAR
brake : Intervention(TRUE, pf_vel!=0
lock_arm : Intervention(arm_pos=1, T
```

```
-- Warning states
DEFINE flag_st_1 := arm_pos = 0 & pf_vel=1;
DEFINE flag_st_2 := arm_pos = 1 & pf_vel=1;
DEFINE flag_st_3 := arm_pos = 1 & pf_vel=2;
------------------------------------------------------------

-- Strategy definition
DEFINE flag_brake := flag_st_2 | flag_st_3 ;
DEFINE flag_lock_arm := flag_st_1 ;
```

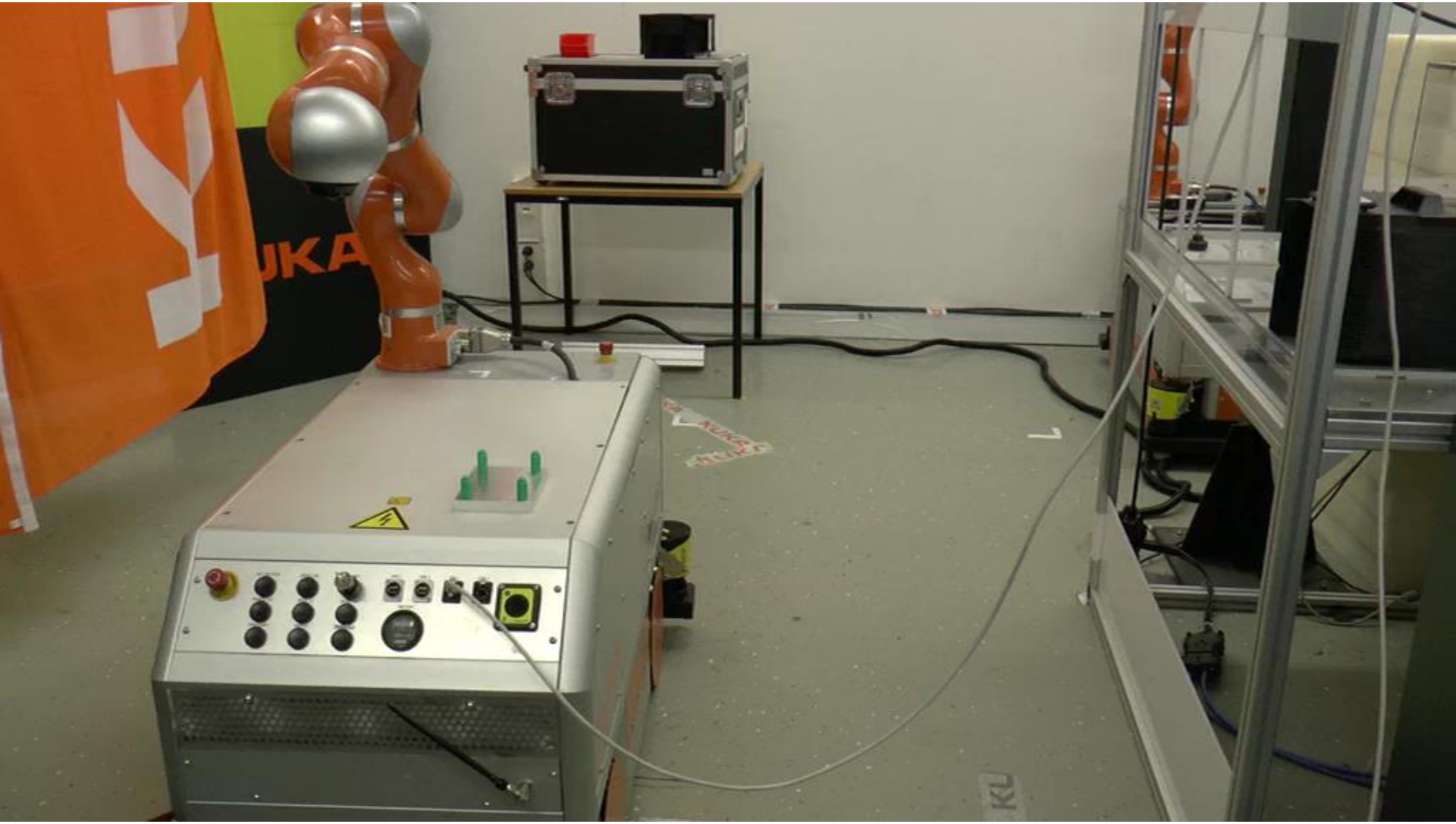
A case study

- Mobile plateform OmniRob with an articulated arm (Lightweight Robot)

- Available interventions:
  - Block the arm
  - Engage the platform brakes
- Hazard analysis with Hazop-UML
  - 100 lines with a non-zero severity
  - 13 invariants, including:

"The robot arm must not be extended beyond the platform footprint when the platform moves."

The safety monitor in action



Conclusion

- Design method for an active safety monitor
  - Off-line specification of the safety rules from the risk analysis
  - On-line interventions to fulfill the rules
- Tool and template to synthesize the safety rules
- Application to industrial case study

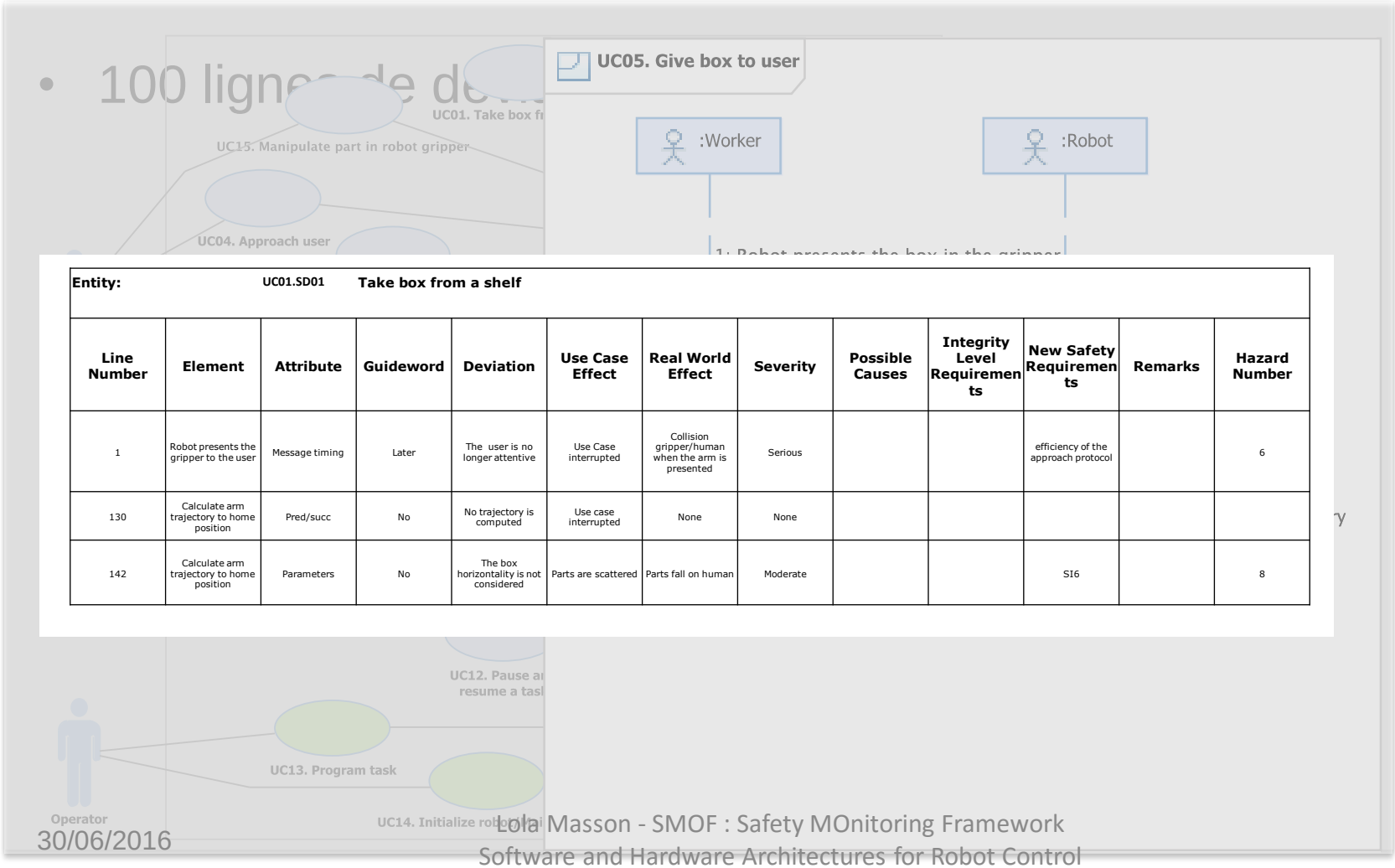
Perspectives

- New case study :
  - Mobile plateform with a static arm supporting a light sensor

- Multi-level monitoring
  - Monitoring at different levels of the software robotic architecture (observations, interventions, …)
  - Multi-margins
  - Multi-level of autonomy

Pré-requis de la méthode

- Analyse de risque HAZOP/UML



Entity:	UC01.SD01	Take box from a shelf										
Line Number	**Element**	**Attribute**	**Guideword**	**Deviation**	**Use Case Effect**	**Real World Effect**	**Severity**	**Possible Causes**	**Integrity Level Requirements**	**New Safety Requirements**	**Remarks**	**Hazard Number**
1	Robot presents the gripper to the user	Message timing	Later	The user is no longer attentive	Use Case interrupted	Collision gripper/human when the arm is presented	Serious			efficiency of the approach protocol		6
130	Calculate arm trajectory to home position	Pred/succ	No	No trajectory is computed	Use case interrupted	None	None					
142	Calculate arm trajectory to home position	Parameters	No	The box horizontality is not considered	Parts are scattered	Parts fall on human	Moderate			SI6		8