Autonomous systems are characterized by:
- complex control software, very difficult to verify;
- the ability to operate in unstructured environments;
- versatility, the ability to carry out very different tasks.
Such systems should thus be equipped with means for safety enforcement, called safety monitors, that are:
- verifiable;
- adaptive, i.e., able to adapt enforcement to context;
- maximally permissive in that it should only restrict versatility to the extent necessary to ensure safety.
We focus here on monitor specification, based on Hazop/UML hazard analysis. The specification is composed of safety rules of the form:

if observation then intervention

We distinguish:
- restriction rules, which inhibit certain state changes (e.g., by means of an interlock device or by request filtering);
- initiative rules, which launch actions in order to change the state. Since any such action takes a non-zero time to produce an effect, it has to be anticipated by some safety margin (with respect to time or some other physical variable).

Safety rule synthesis

- 1 restriction rule to forbid the arm to unfold, when the speed is high
- 1 initiative rule to brake if the arm is unfolded

Graphical method

Not scalable for many variables

=> Use of formal methods

Iteratively, by Model-checking NuSMV, Uppaal

Safety rules for all the hazards

Check consistency

- Check for simultaneous and contradictory interventions by model-checking
- Requires synchronization of variables common to several hazards

Check consistency

Final set of Safety rules

Check for safety rules

Yes

No

End

Check Versatility

Set intervention

Remove intervention

Supervisor Synthesis

- System as automata
- Specification as automata
- Permissiveness included
- Control: Enable transitions

Game Theory

- System as automata
- Specification as CTL property
- Safety and liveness properties
- Control: Fire transitions

EADS-Astrium