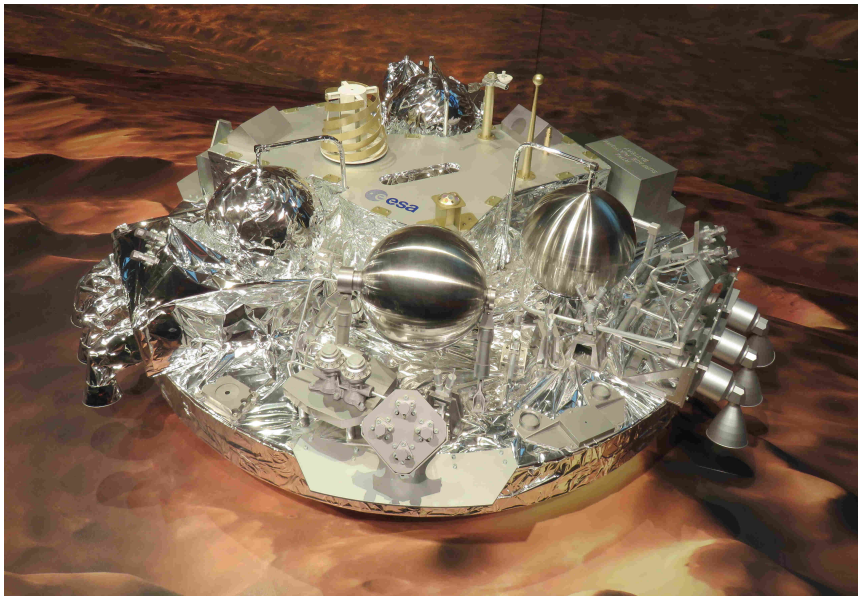
La vérifiation formelle pour assurer la sureté des systèmes cyber-physiques

Uli Fahrenberg

EPITA Rennes

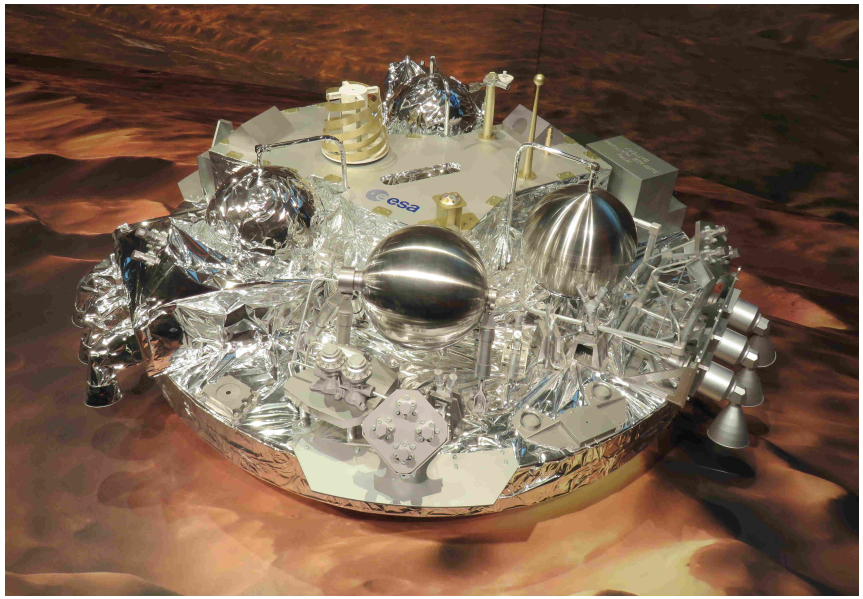
Schiaparelli

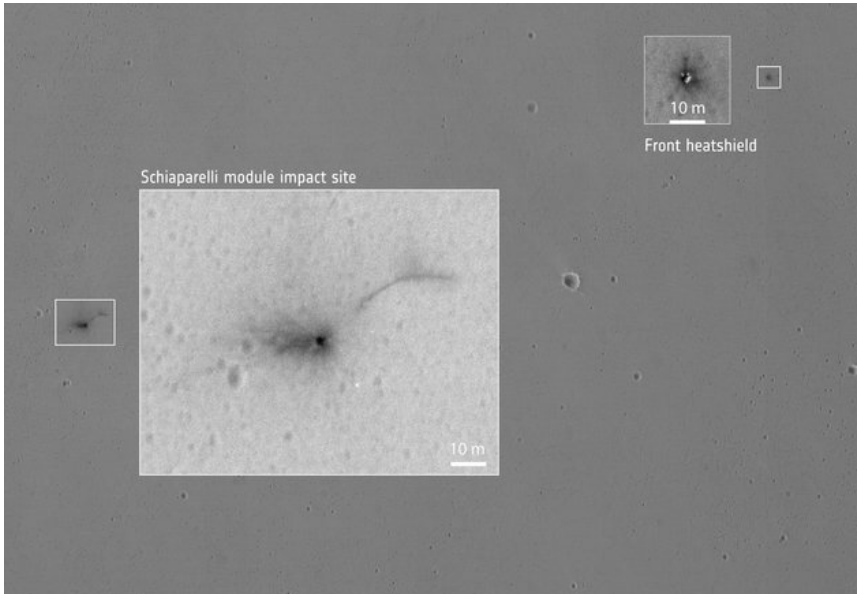
Atterrisseur expérimental ESA / Roscosmos



Schiaparelli

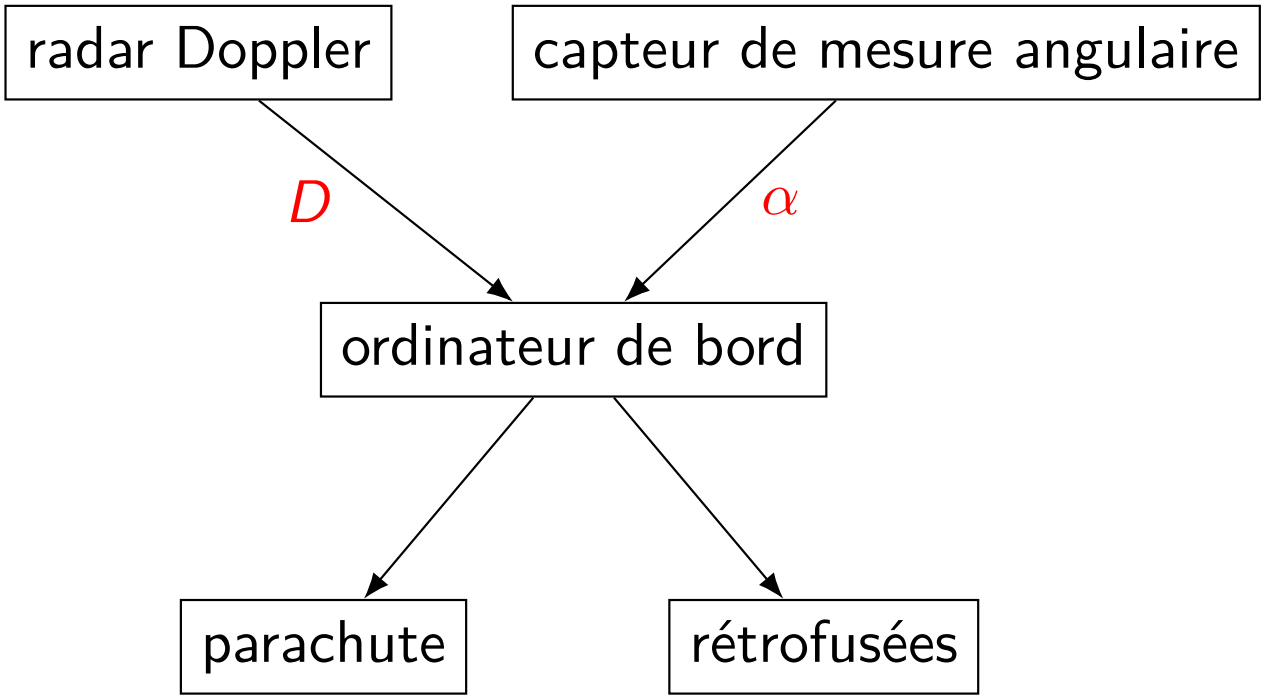
Atterrisseur expérimental ESA / Roscosmos

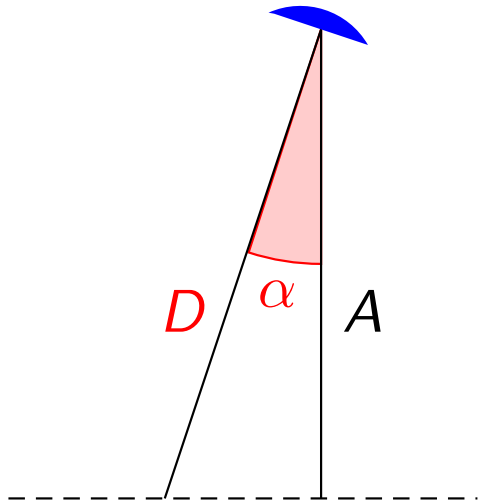




- un exemple d'un système cyber-physique

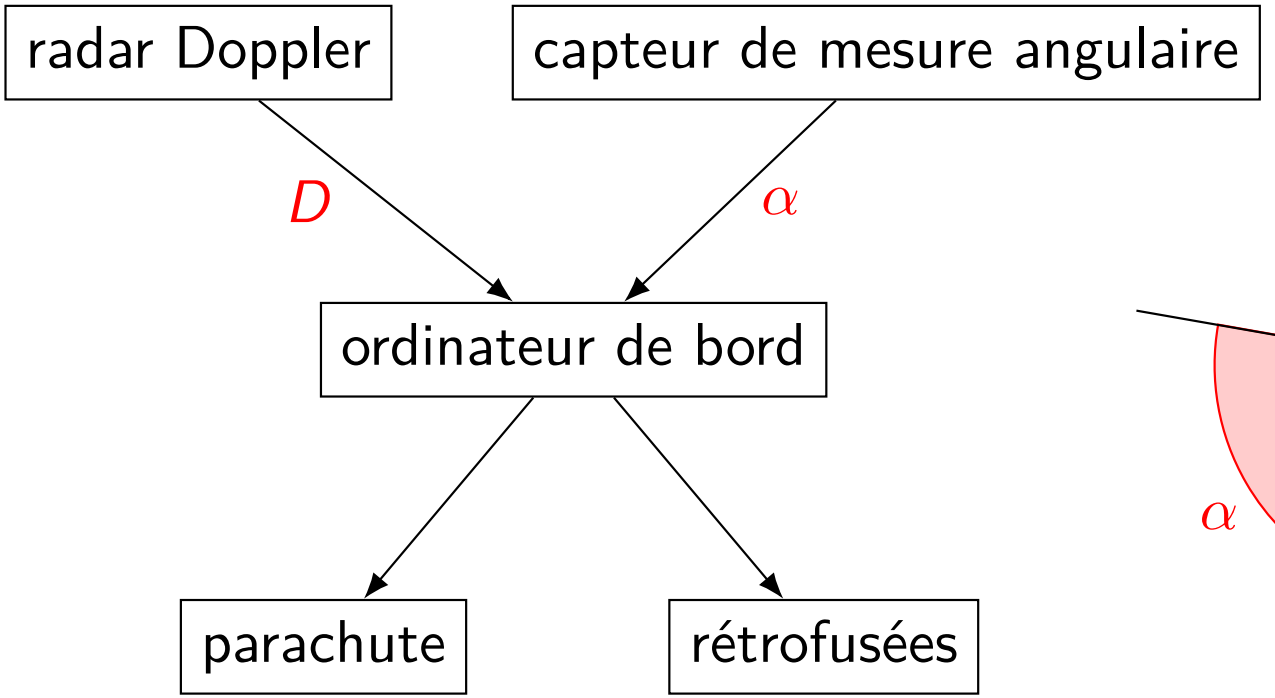
Schiaparelli
Schématique

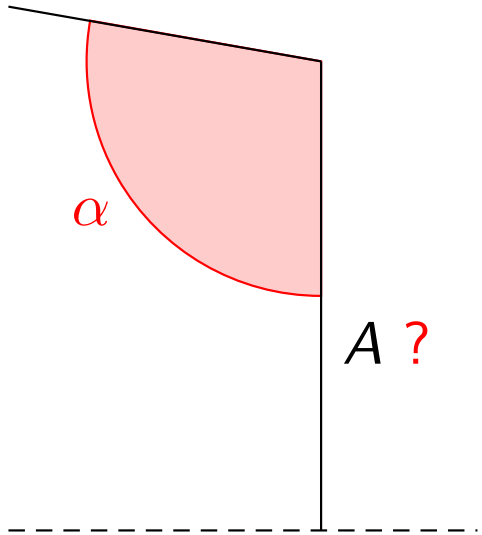




$$A = D \cdot \cos(\alpha)$$

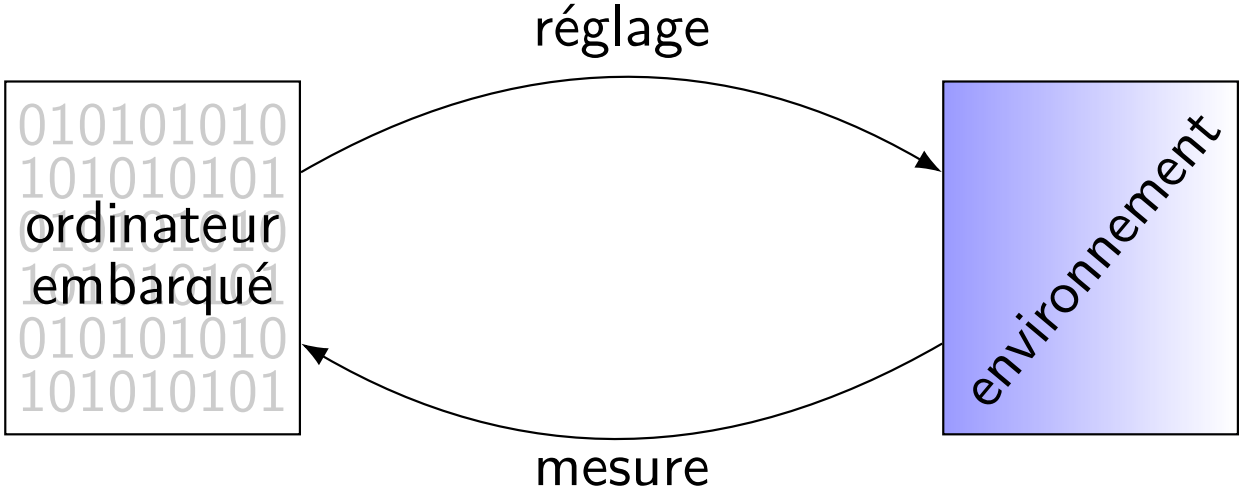
Schiaparelli
Schématique

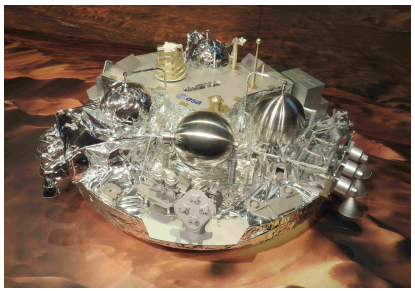


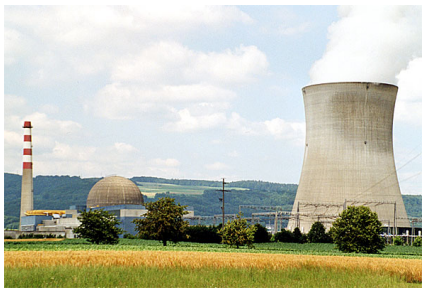


$$A = D \cdot \cos(\alpha)$$

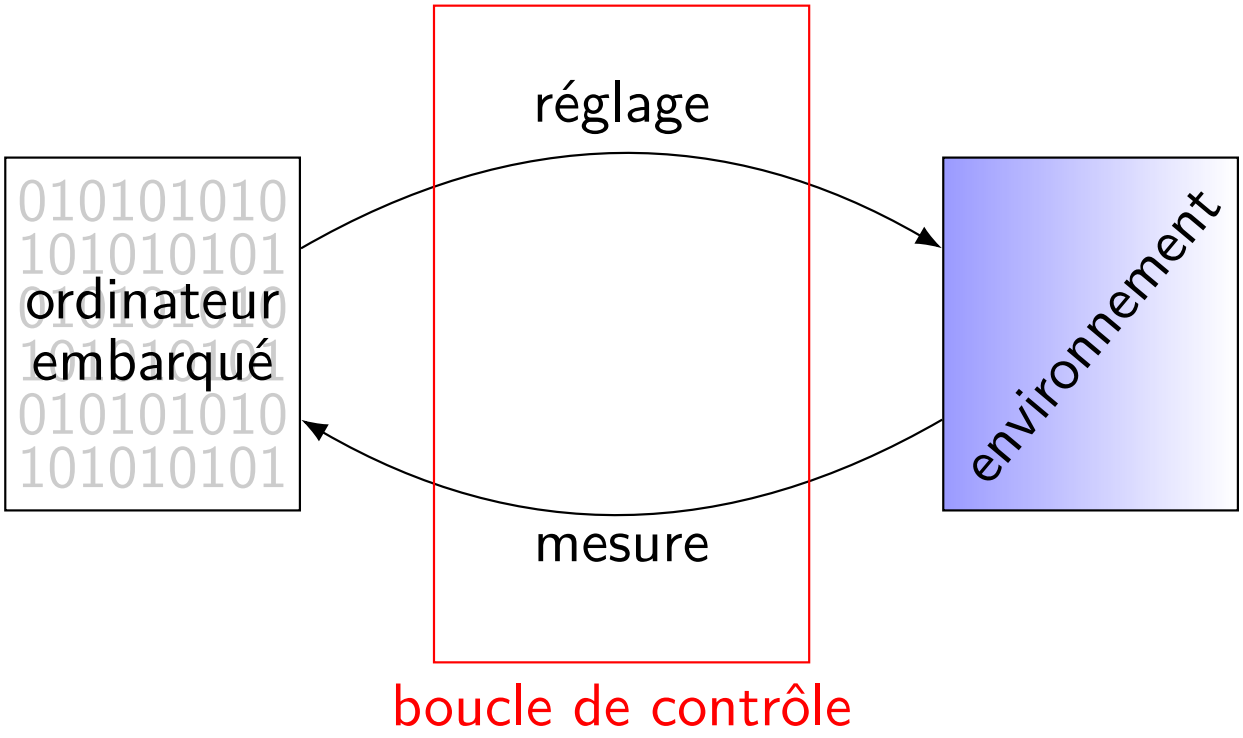
Systèmes cyber-physiques
Exemples



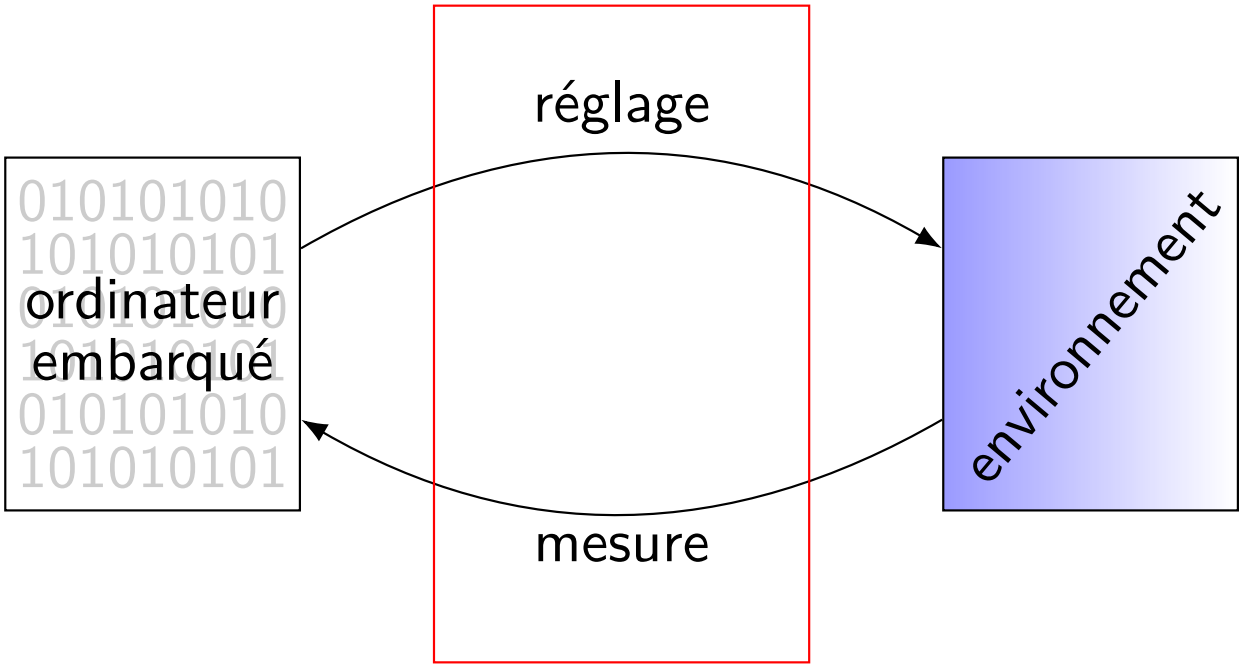




Systèmes cyber-physiques
Schématique

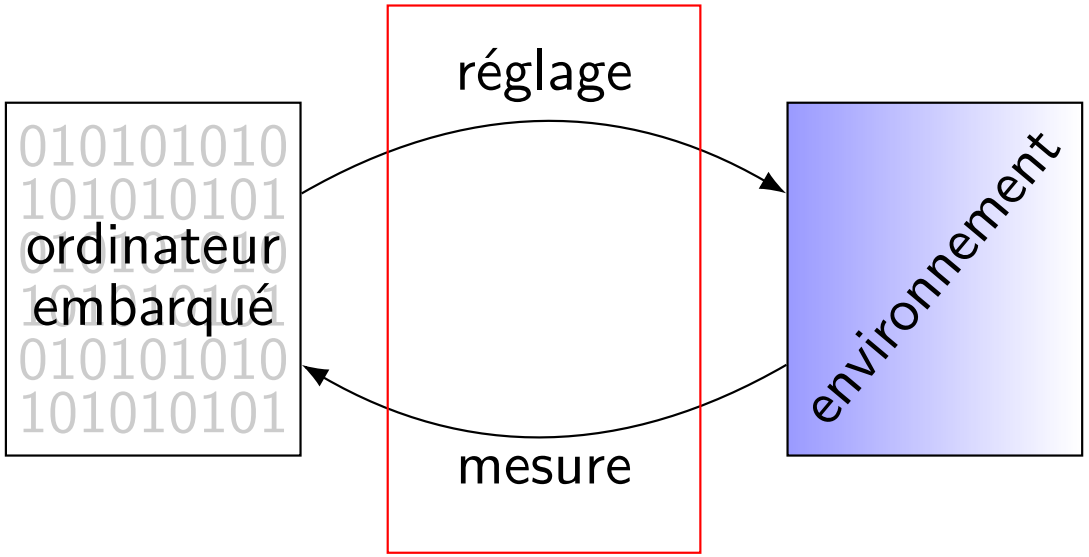


Systèmes cyber-physiques
Schématique

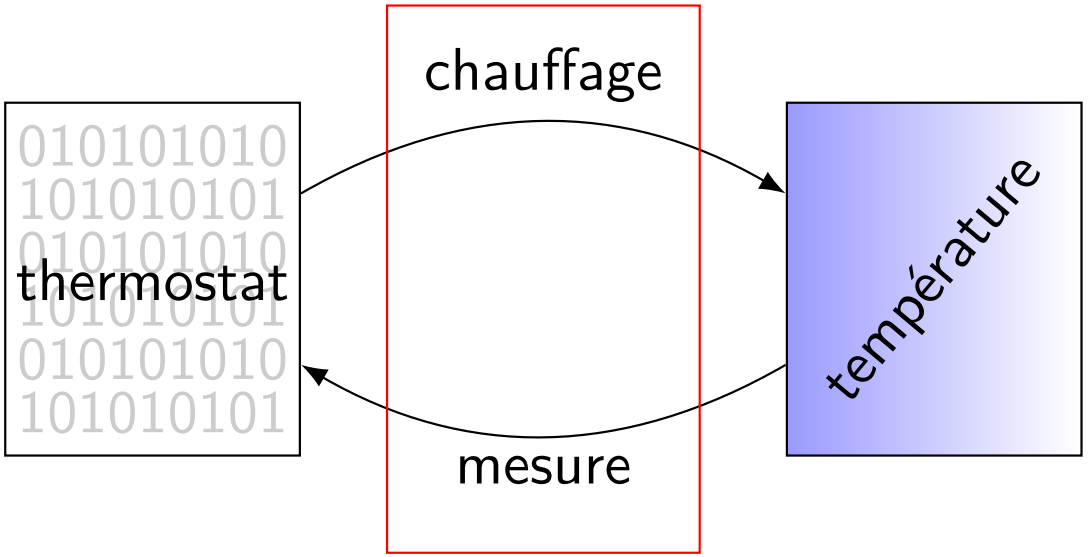


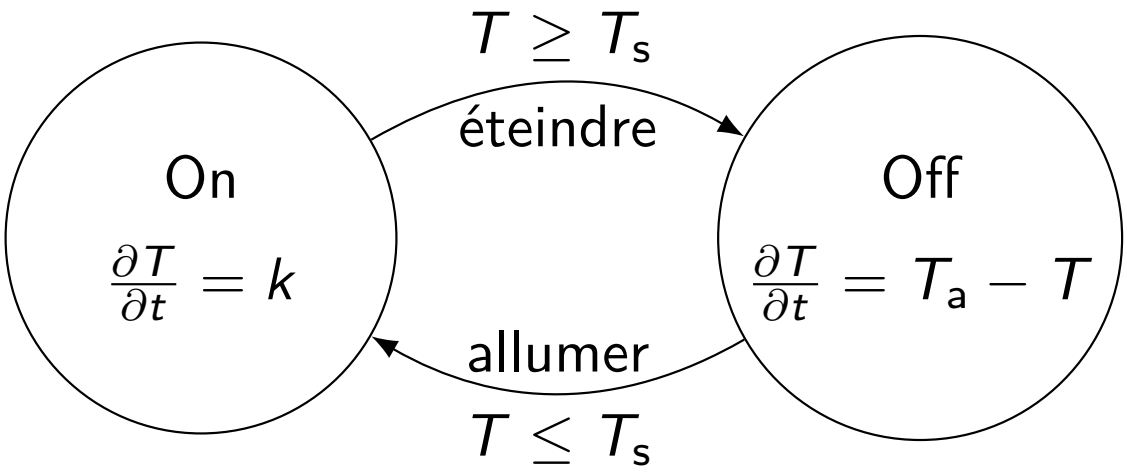
Informatique Théorie du contrôle Mathématiques Physique

Modèle mathématique
d'un thermostat



Modèle mathématique
d'un thermostat

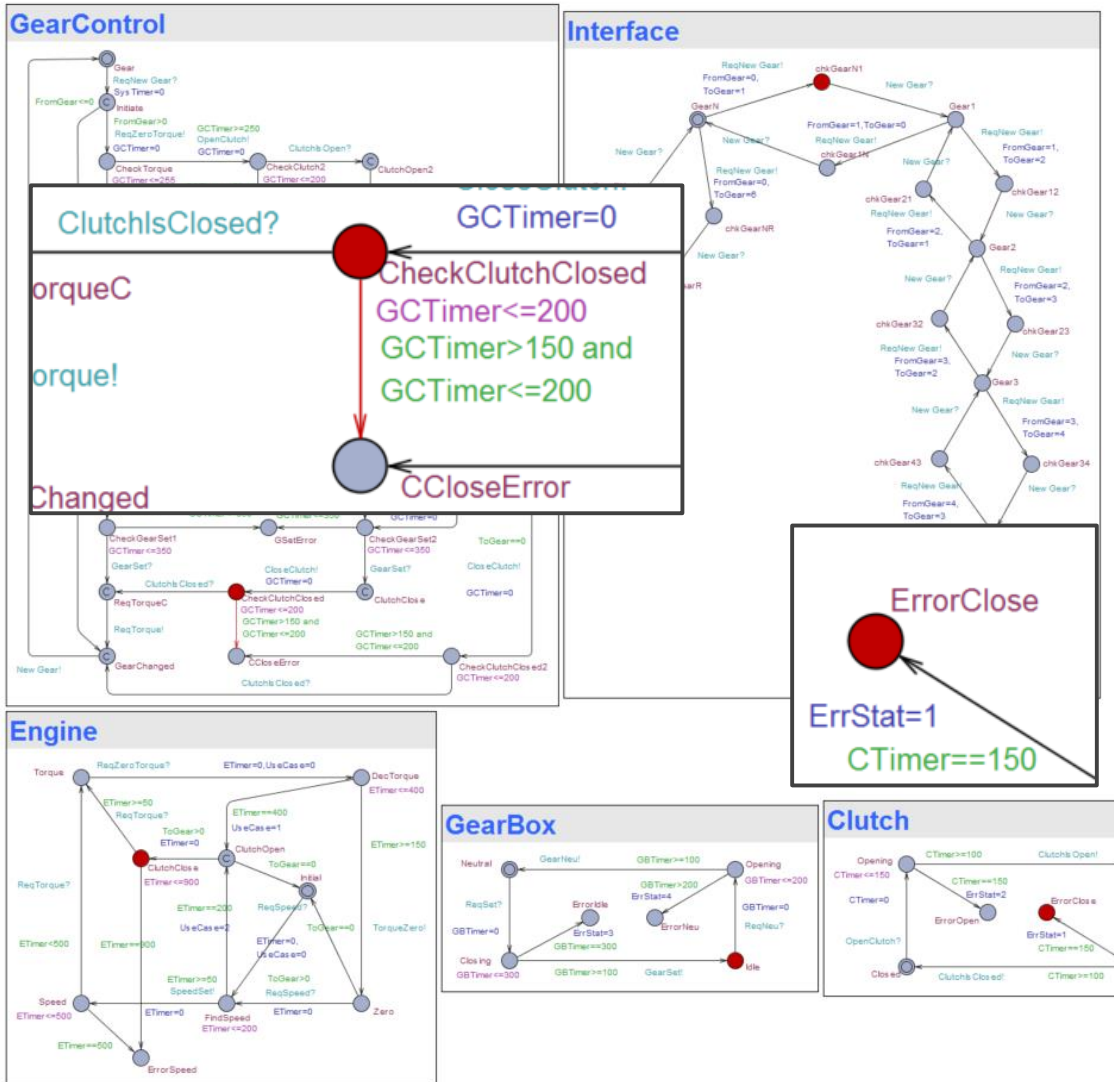




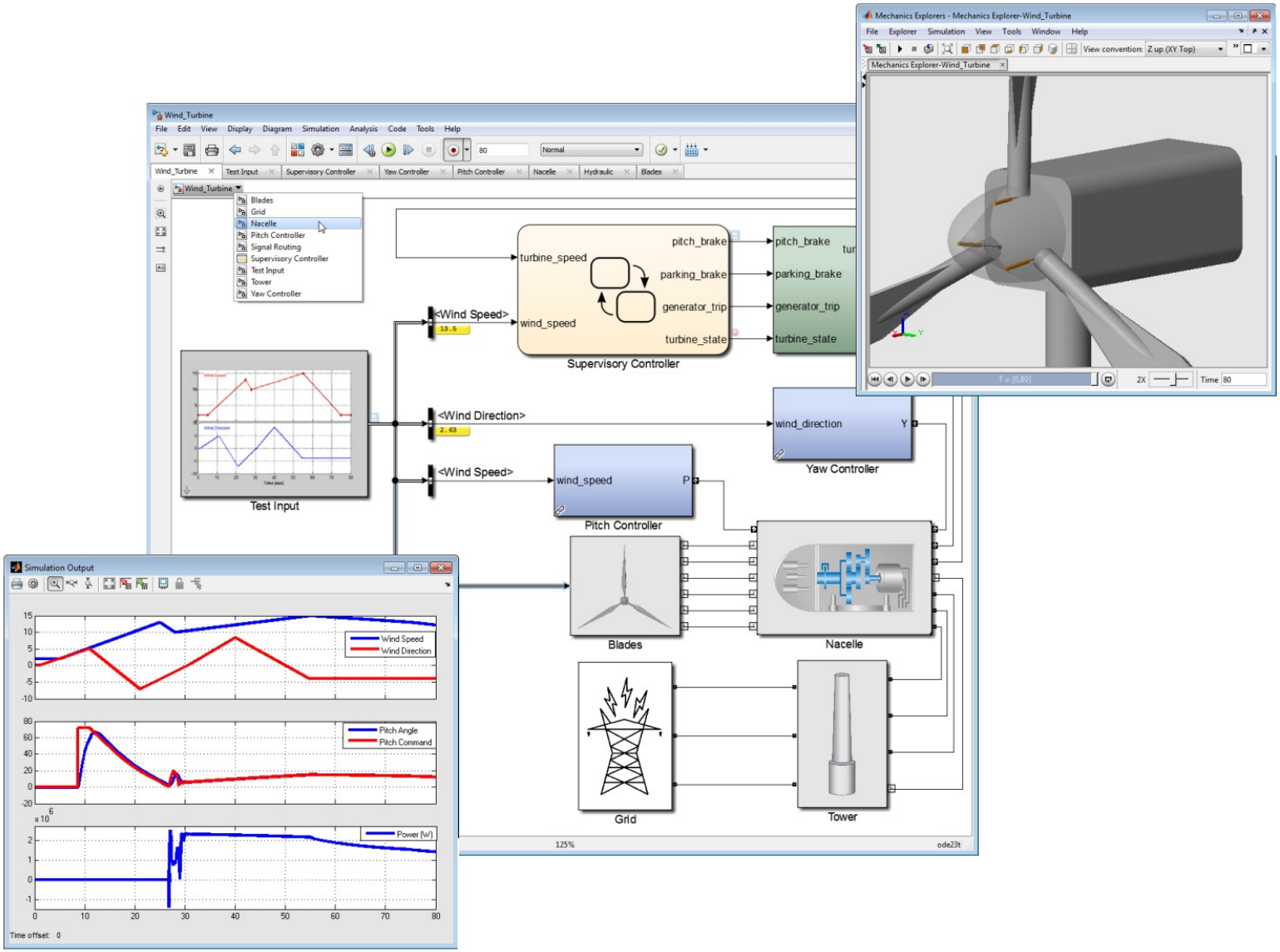
Timed Automata
UPPAAL

- <Global variables>
  - UseCase = 0
  - FromGear = 0
  - ToGear = 0
  - ErrStat = 0
- <Constraints>
  - CTimer ≥ 0
  - ETimer ≥ 0
  - GBTimer ≥ 0
  - GCTimer ≥ 0
  - SysTimer ≥ 0
  - GearControl.GCTimer ≥ 0
  - CTimer = ETimer
  - ETimer = GBTimer
  - GBTimer = GCTimer
  - GCTimer = SysTimer
  - SysTimer = GearControl.GCTimer
  - GearControl.GCTimer = CTimer

Timed Automata Models

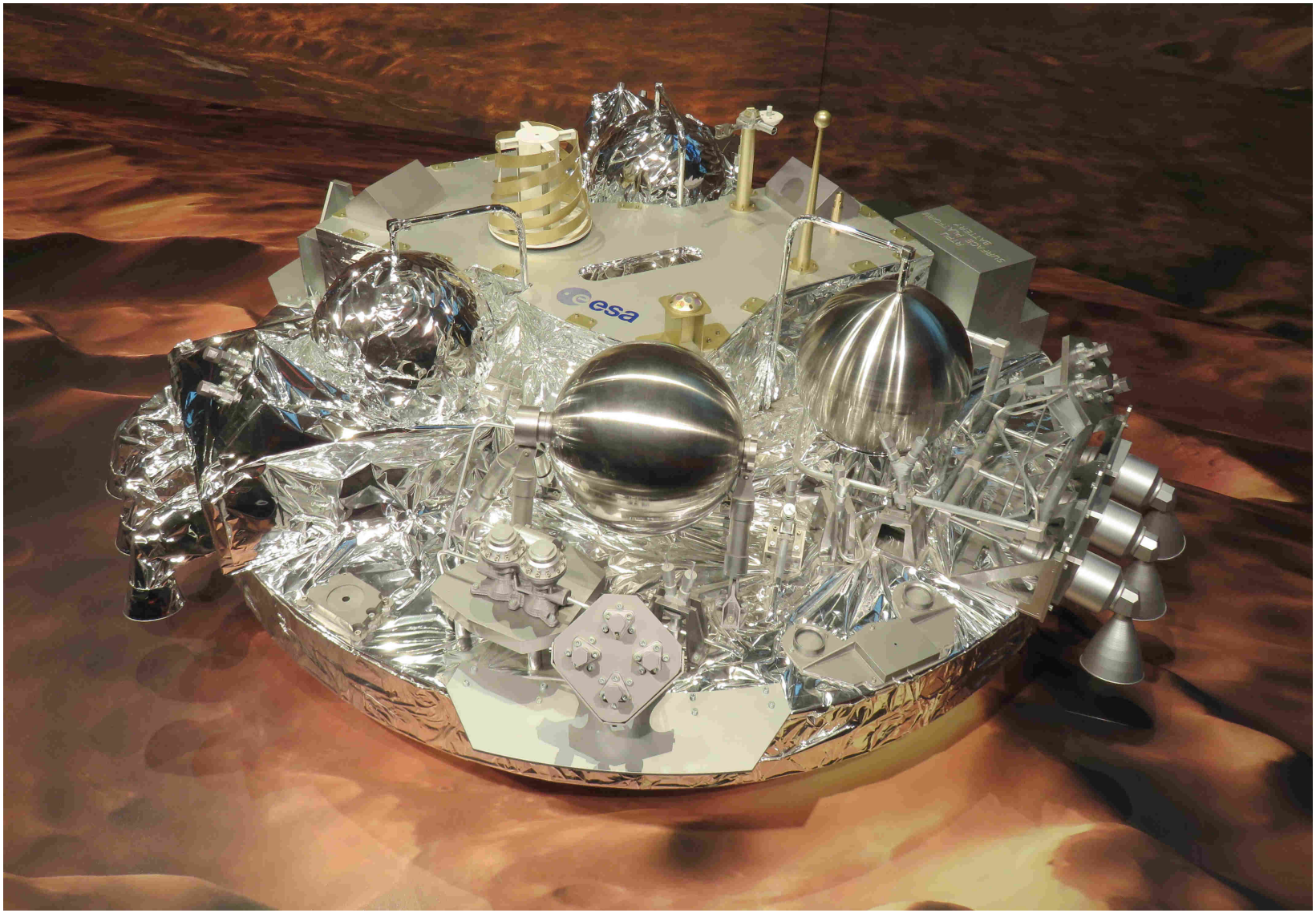


Modèle Simulink
d'une éolienne



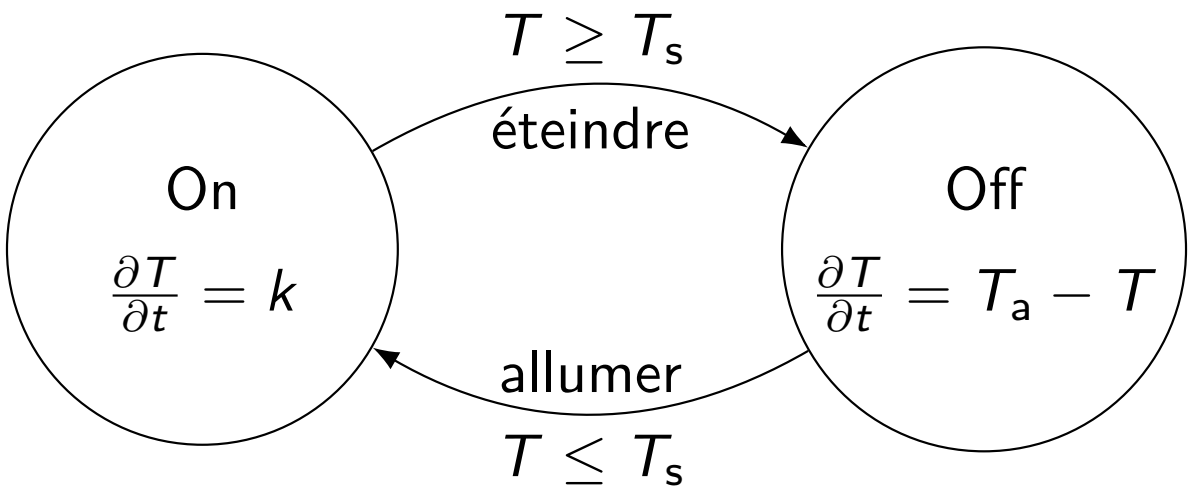
Schiaparelli

De l'insuffisance de la simulation d'un modèle

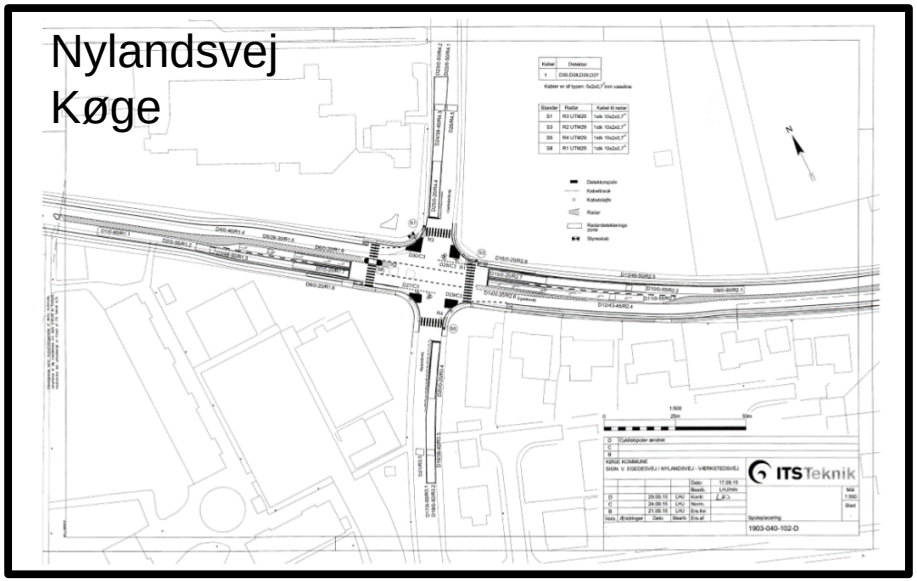


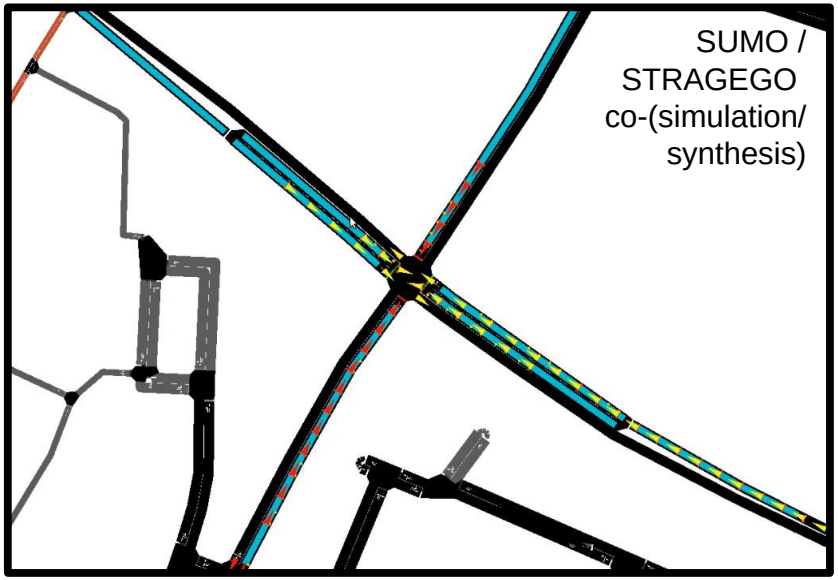
La vérification formelle

S'assurer des propriétés au-delà de la simulation



UPPAAL Stratego
pour contrôle de la circulation





Scenario	Static		Loop Induction		Stratego		Imp W time over LI %
	Jam Km	W time s	Jam Km	W time s	Jam Km	W time s	
MAX	1451	191990	1185	157200	551	73001	53.5%
MID	456	60362	369	48936	331	43878	
LOW	138	18425	139	18566	101	13451	27.5%

Scenario:
2 hours traffic

La vérification formelle des systèmes cyber-physiques
dans le monde

La vérification formelle des systèmes cyber-physiques
en France

- IRISA, Rennes
- Verimag, Grenoble
- ENSTA Brest
- École polytechnique, Palaiseau
- Télécom ParisTech, Palaiseau
- Isae-Supaéro, Toulouse
- ...

Aussi un problème cyber-physique

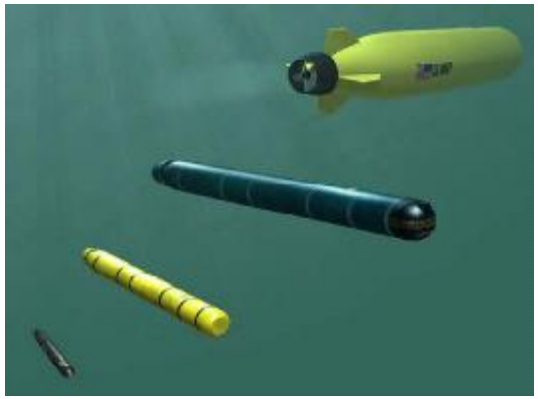
Meltdown

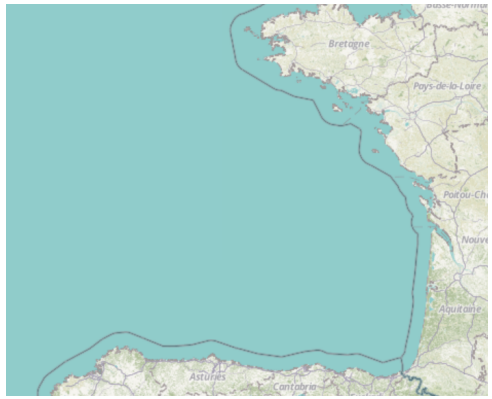
Spectre

Conclusion

La vérifiation formelle pour assurer la sureté des systèmes cyber-physiques

- système cyber-physique : système informatique embarqué qui interagit avec son environnement physique
- pour assurer la sureté des systèmes cyber-physiques : la simulation
- vérification formelle pour aller plus loin
- mon intérêt : vérification formelle des systèmes cyber-physiques distribués
- exemple : meute de sous-marins autonomes qui explorent une baie





Remerciements : Éric Goubault, Kim Larsen, Luc Jaulin, Chloé Aubisse-Daniault et Aline Fahrenberg