Dealing with uncertainty in safety-critical cyber-physical systems

A control engineering perspective

dr. ir. Sofie Haesaert

Assistant Professor
TU Eindhoven

November 27, 2019

Control engineering — classically

Provide stability, performance and robustness via feedback withstanding physical uncertainty and stochasticity

Mechanical ~1788
Governor & throttle valve
1st automatic control

Analogue
PID control

Digital control
Optimal control
Robust control
Complex systems

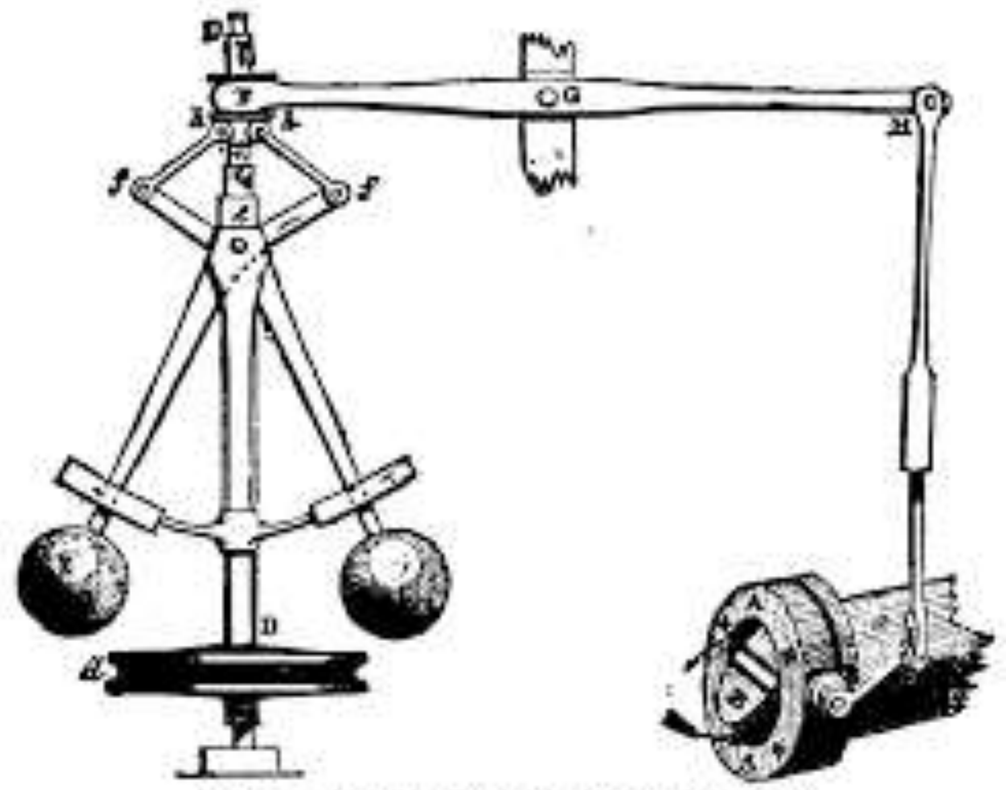
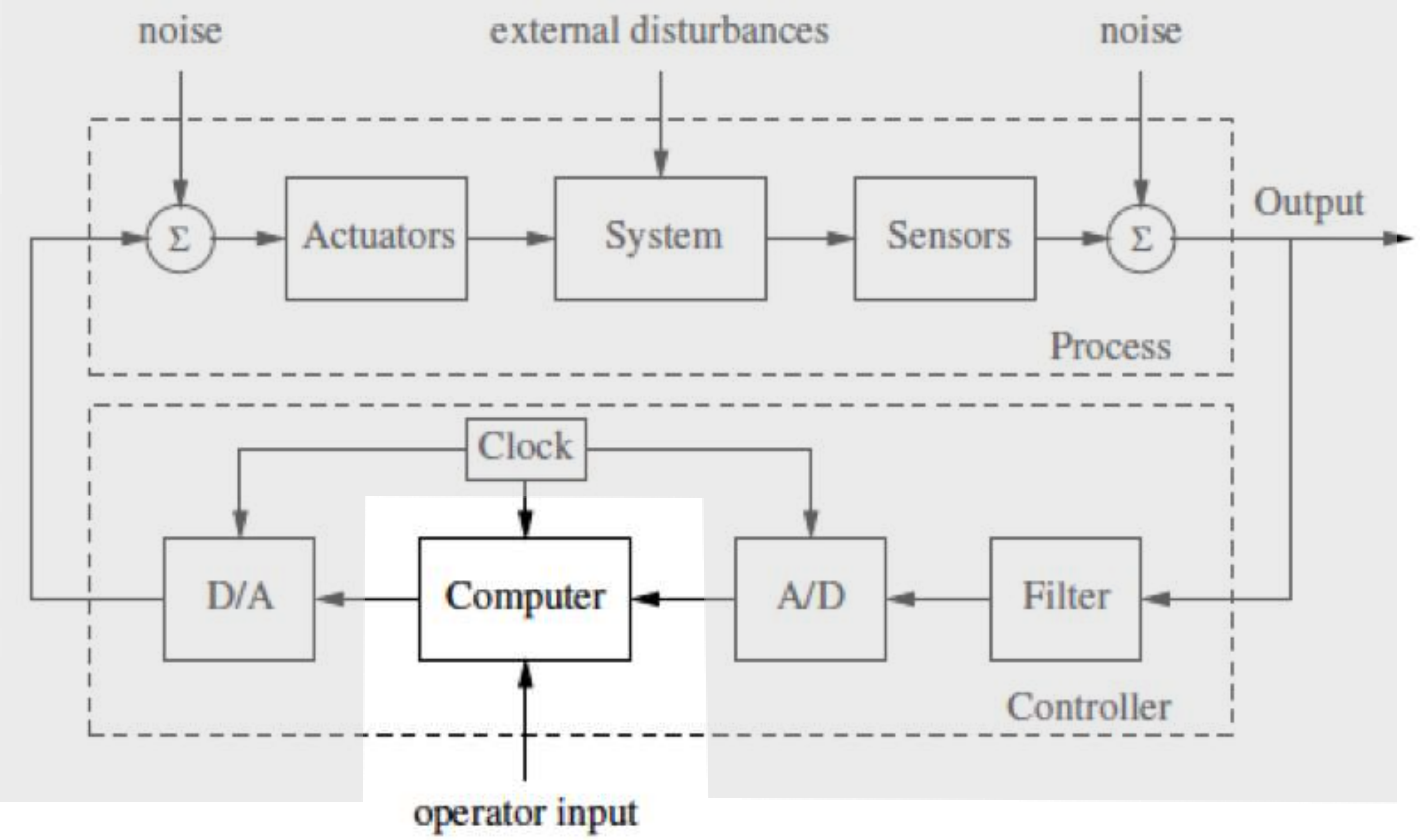


FIG. 4.—Governor and Throttle-Valve.

Examples of digitally controlled systems



Models for digital control

state: $x(t+1) = F(x(t), u(t))$ **+disturbances**

output: $y(t) = H(x(t), u(t))$ **+ sensor noise**

Dynamical systems modeled via ordinary differential equation

state: $\dot{x}(t) = f(x(t), u(t))$ **+disturbances**

output: $y(t) = h(x(t), u(t))$ **+ sensor noise**

Control engineering — emerging

Waymo's fully autonomous driving

Technological innovations lead to increased functionality, complexity and autonomy

Credit: waymo.com

Cyber-physical systems (CPS)

Complex merging of computation into the physical world

Increase of connectivity, functionality, complexity, and autonomy

Physical systems with software for communications, interactions, sensing, and control.

Delivery drones (amazon)

Credit: dryve.com

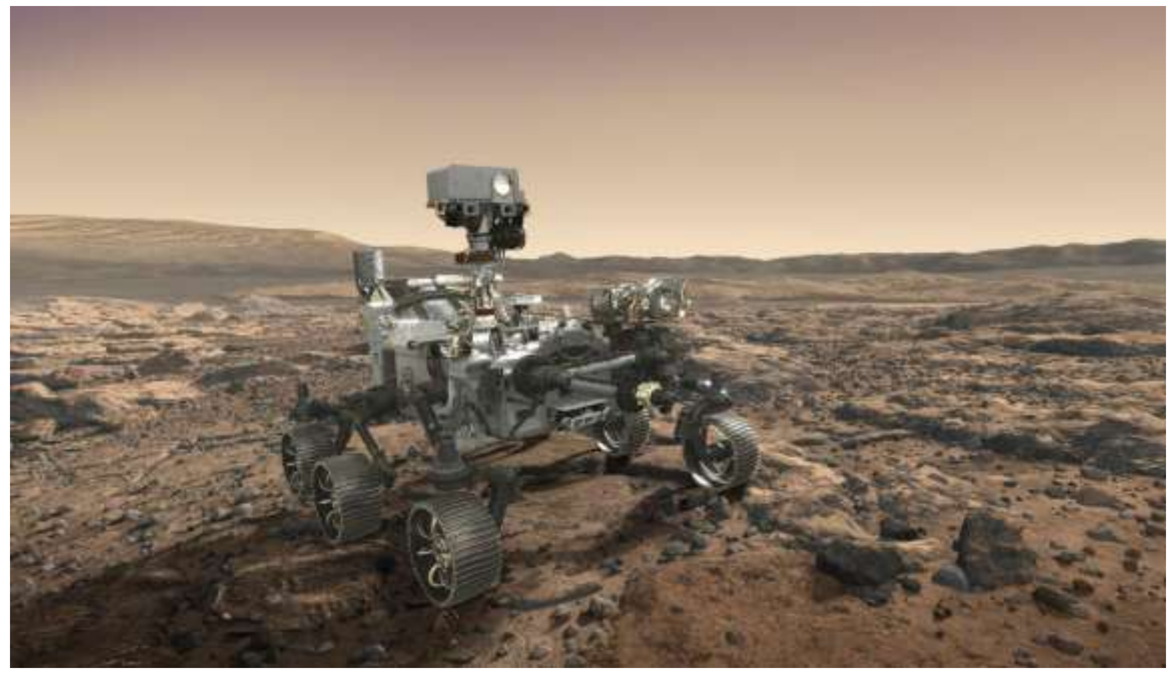
Autonomous driving

Credit: Amber

Smart grid

Credit: unsplash

Long-term autonomy on Mars rover missions



Credit: NASA/JPL-Caltech

Safety-critical cyber-physical systems

Complex merging of computation into the physical world

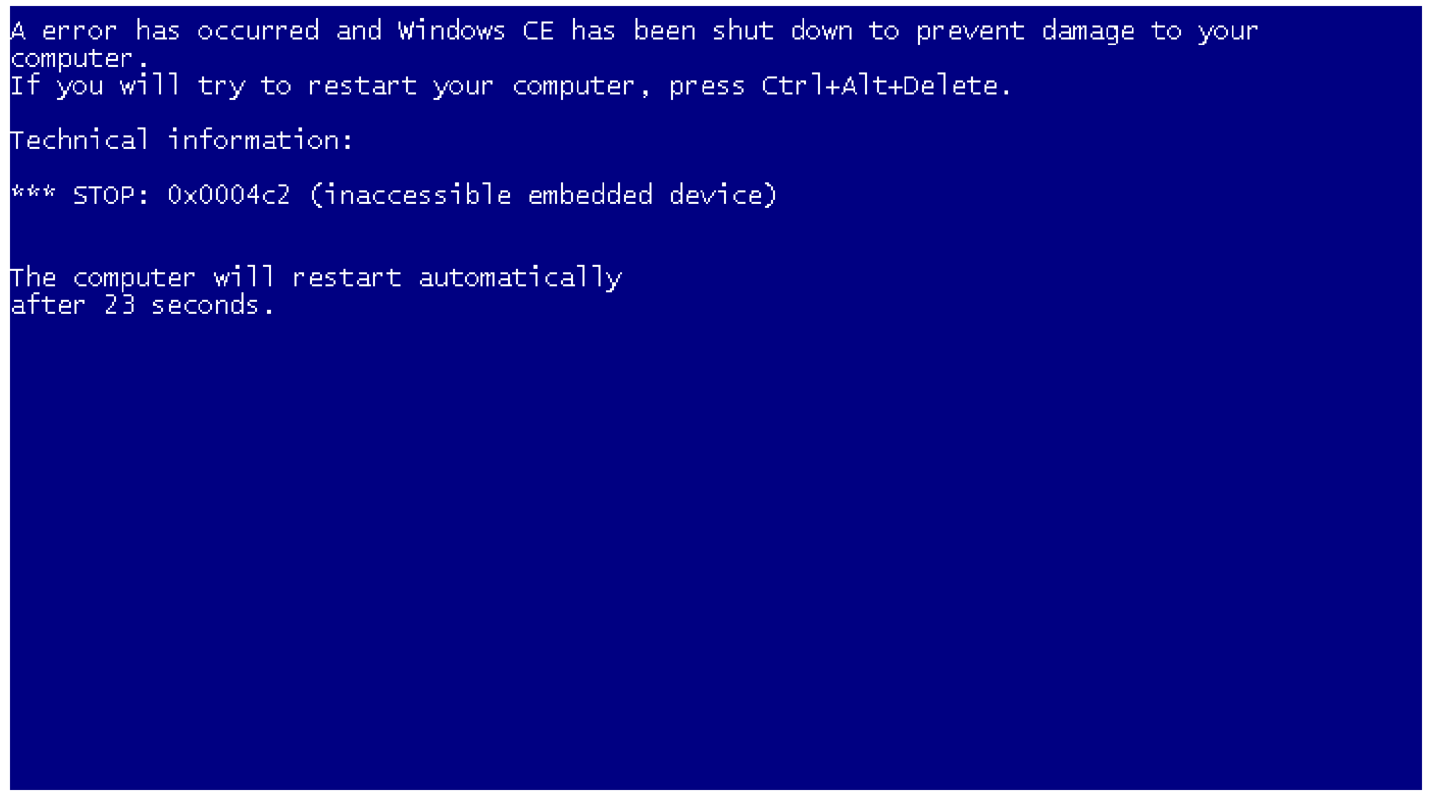
Increase of connectivity, functionality, complexity, and autonomy

Physical systems with software for communications, interactions, sensing, and control.

Software bugs directly affect physical world

Verify software + physical system

- Uncertain, continuous space models
- Noisy output measurements
- Stochastic disturbances

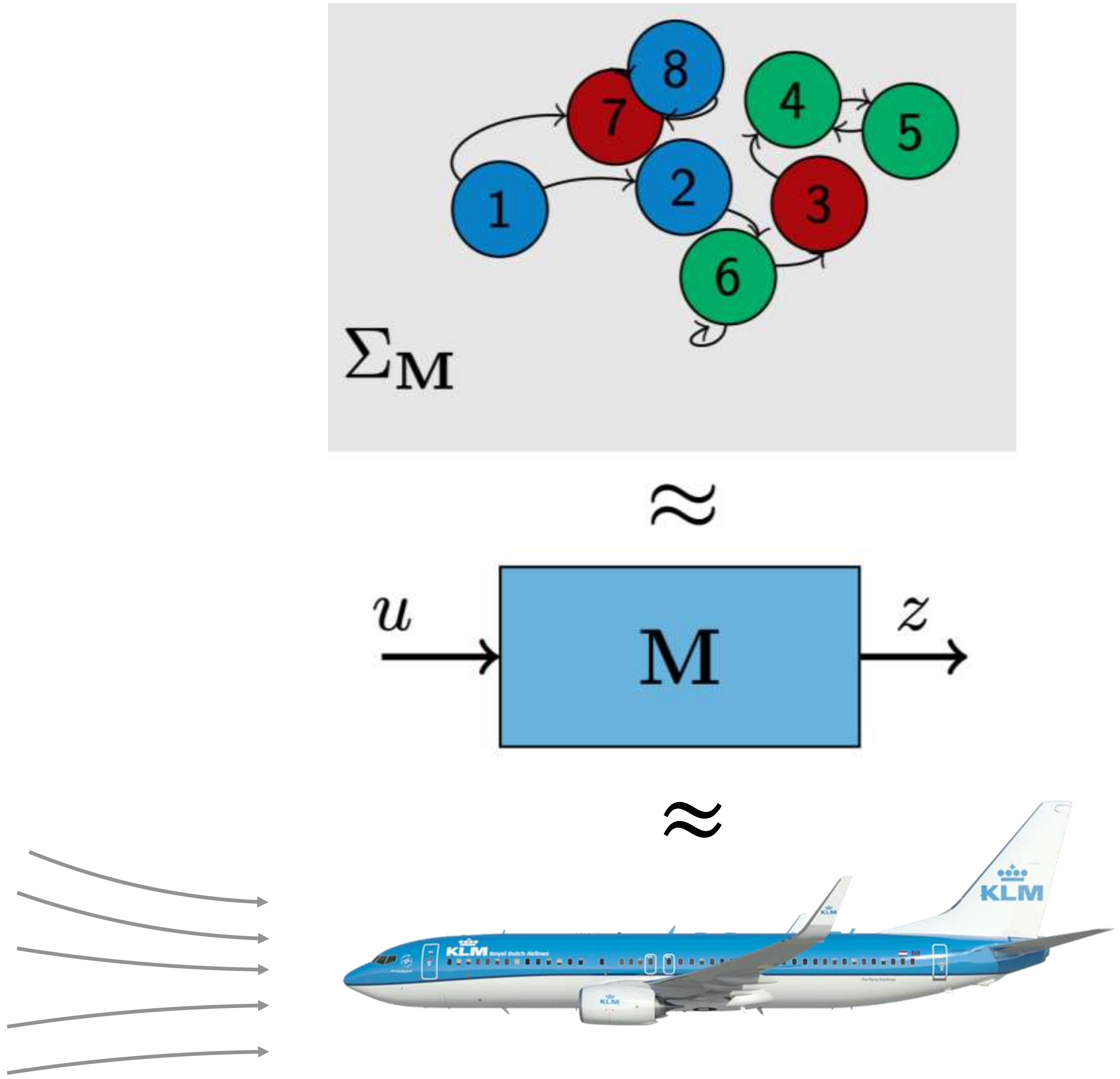


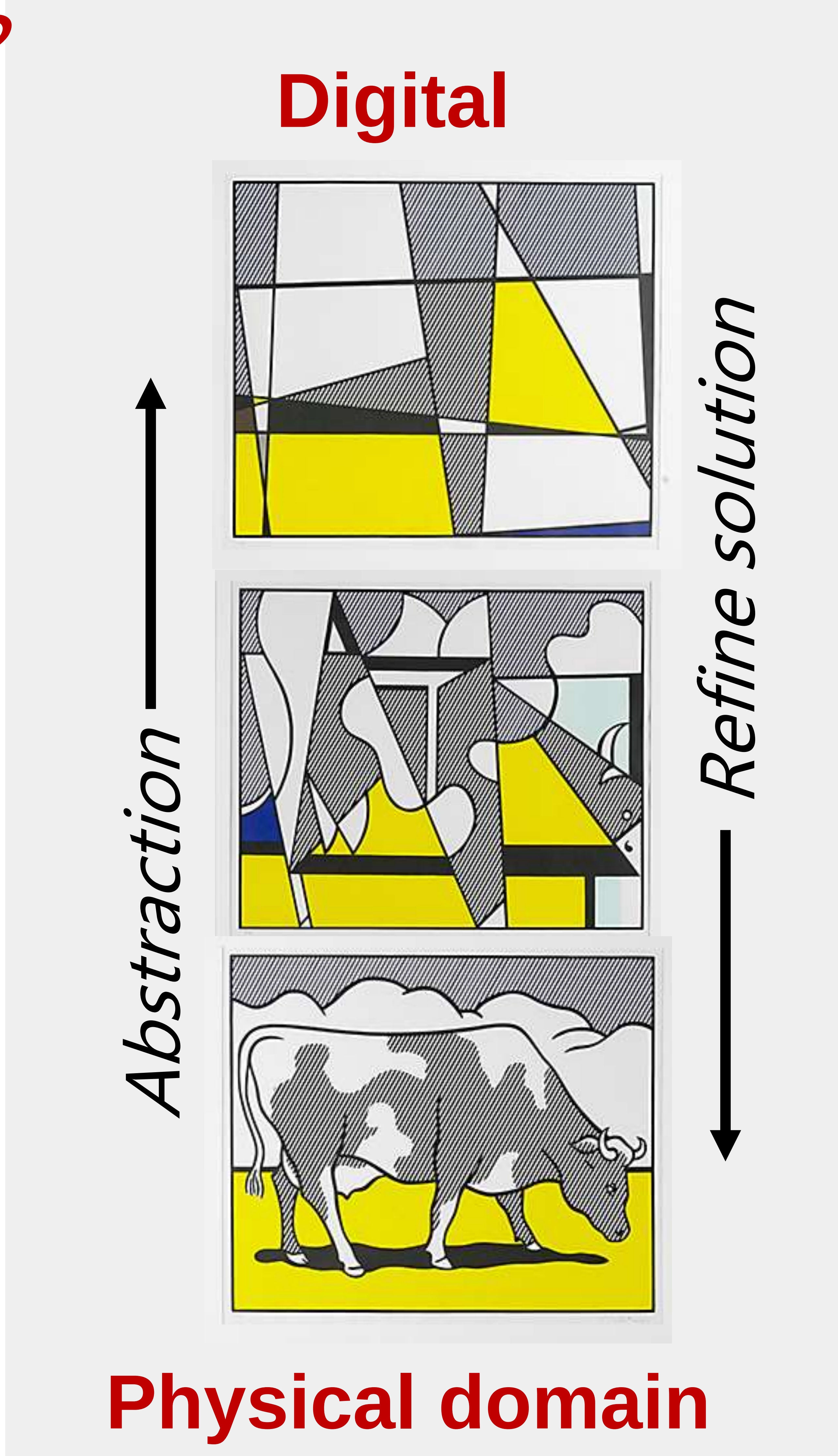
Dealing with stochasticity in CPS

How to design and verify digital control?

High-level specifications
e.g., Avoid ***A*** *until* ***K*** *and*
eventually visit **L** …

Physical model
- Wind & temperature
- Component failure
- Human behavior



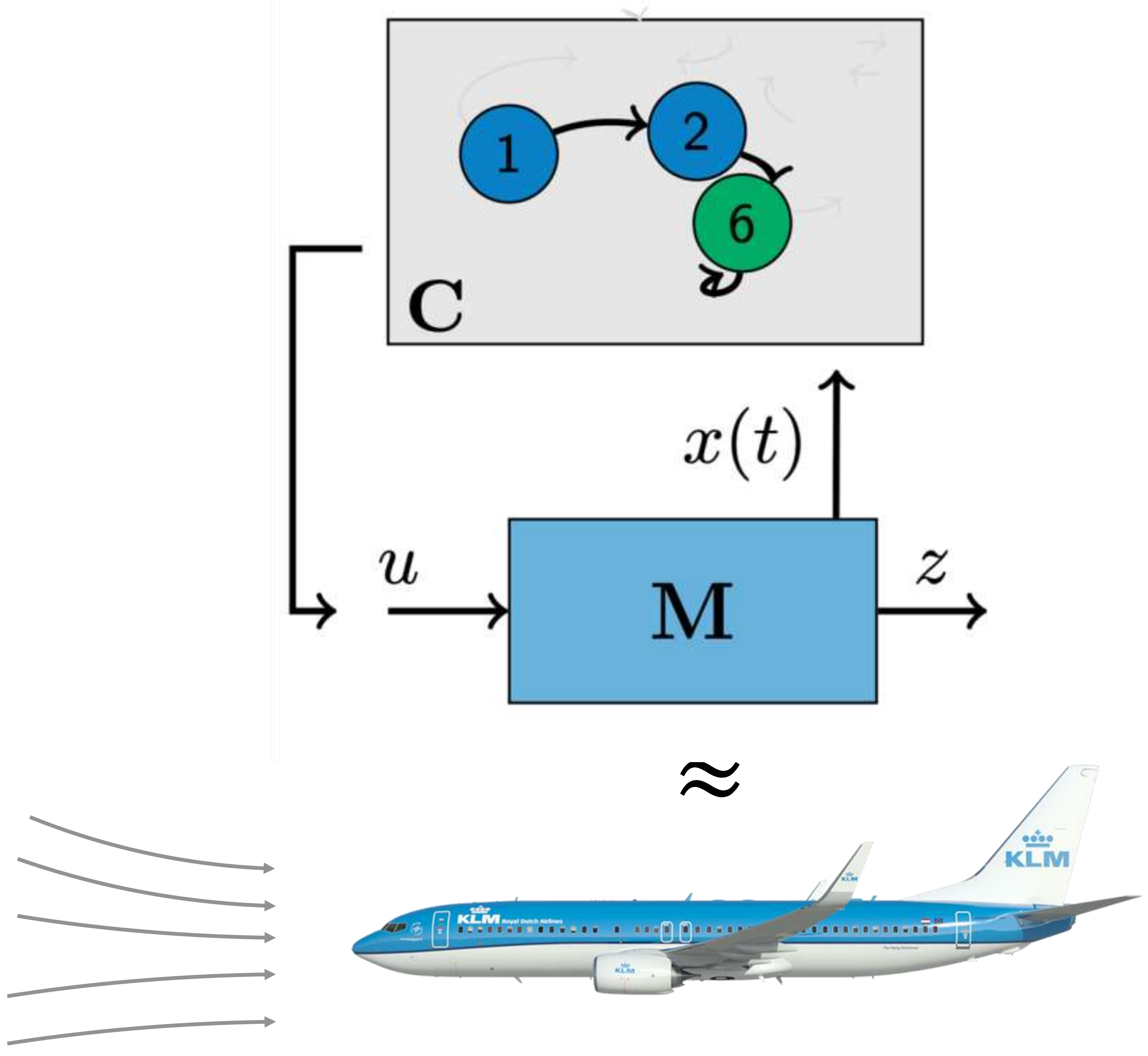


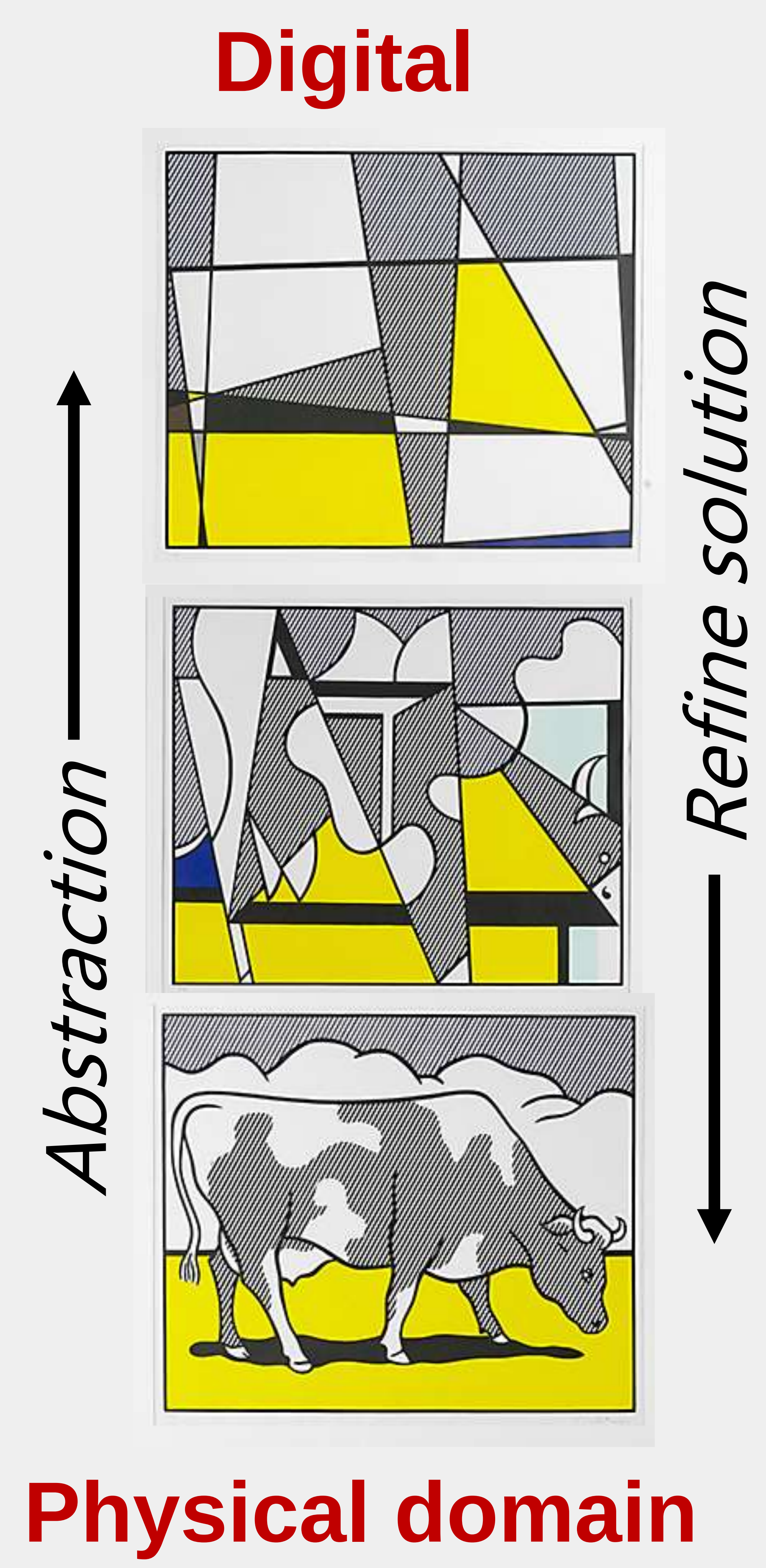
Dealing with stochasticity in CPS

How to design and verify digital control?

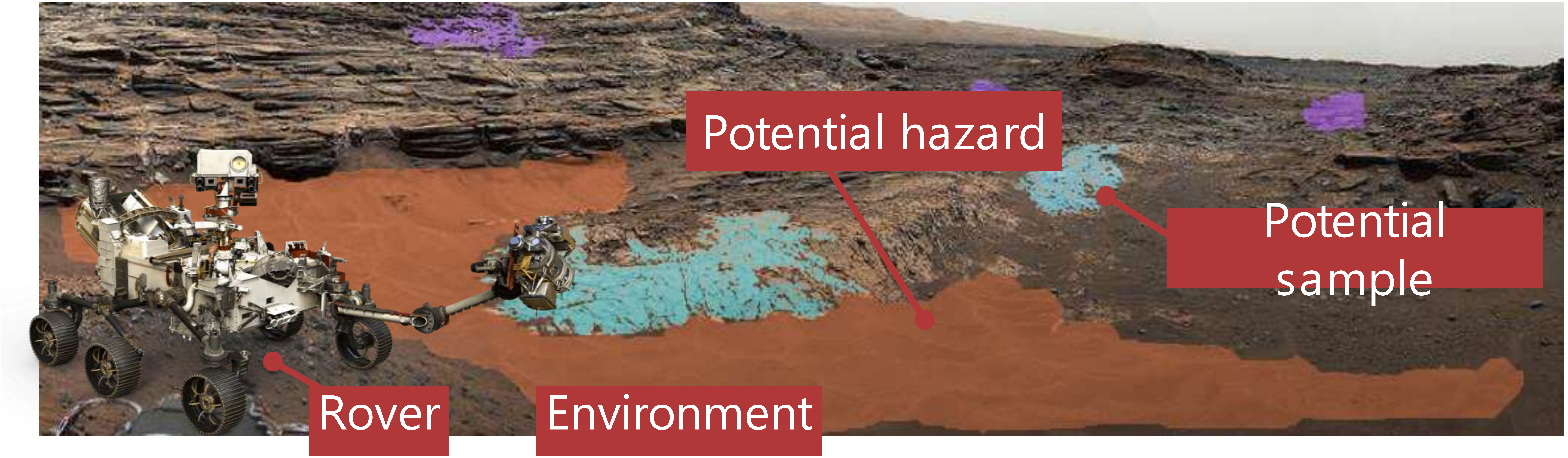
High-level specifications
*e.g., Avoid **A** until **K** and*
eventually visit **L** …

Physical model
- Wind & temperature
- Component failure
- Human behavior





Dealing with partial & noisy observations



Mission specification

$\psi := \neg \text{fail}\, \mathcal{U}\, \text{sample}$

Partially observable MPD

$x_{t+1} \sim \mathbb{T}(\cdot | x_t, u_t) \leftarrow$ state

$z_t \sim \mathbb{R}(\cdot | x_t, u_t) \leftarrow$ observations

Belief MDP

$b_t = \mathbb{P}(dx_t \mid (u_k, y_k)_{k \leq t}) \leftarrow$ state

$b_{k+1} \sim \mathbb{T}_b(\cdot | b_k, u_k) \leftarrow$ belief transitions

Abstract problem

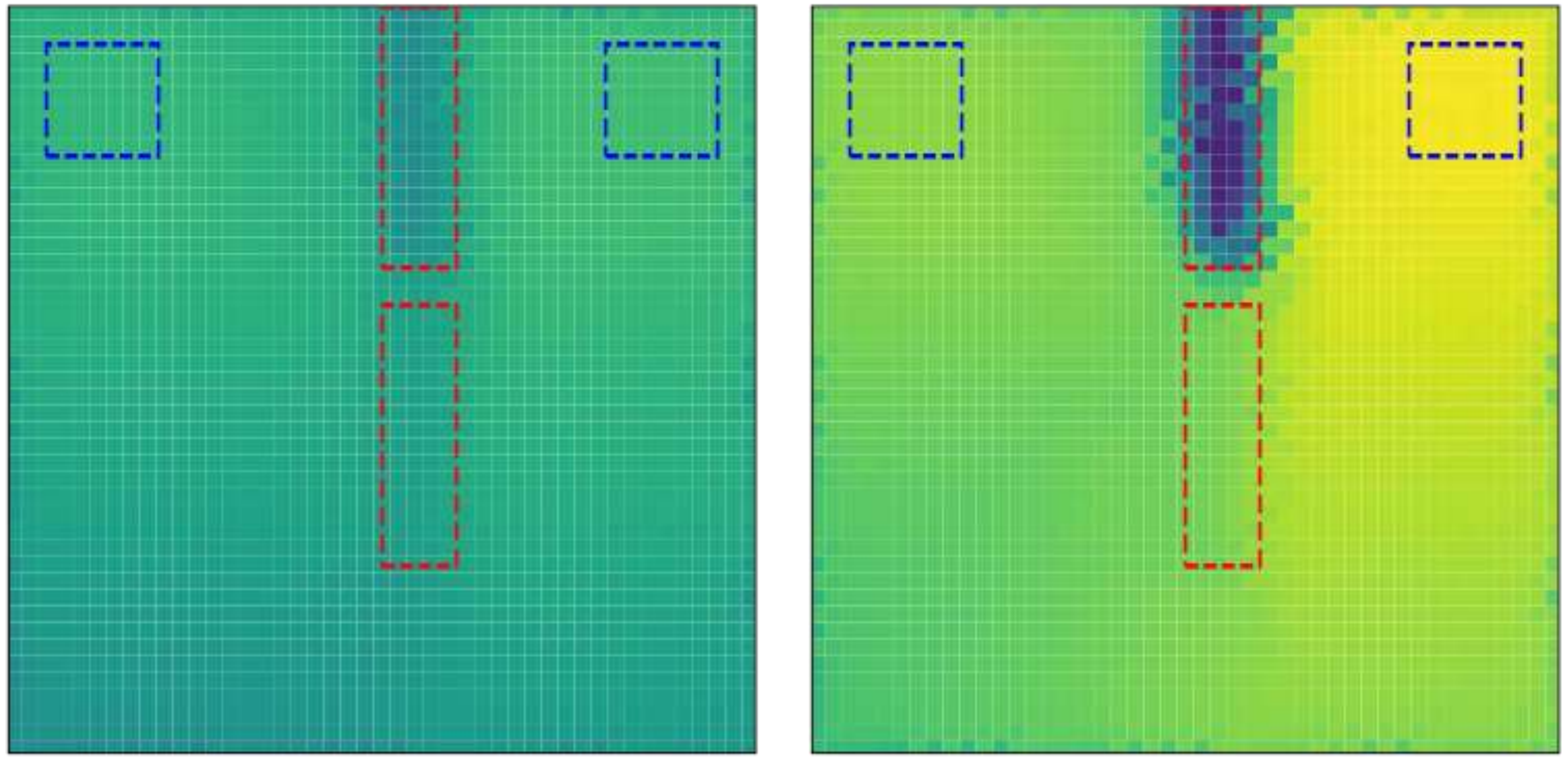
Finite MDP $\tilde{\mathbf{M}}$

$+$ specification ψ

S.Haesaert, P. Nilsson, et. al., ADHS conf. 2018

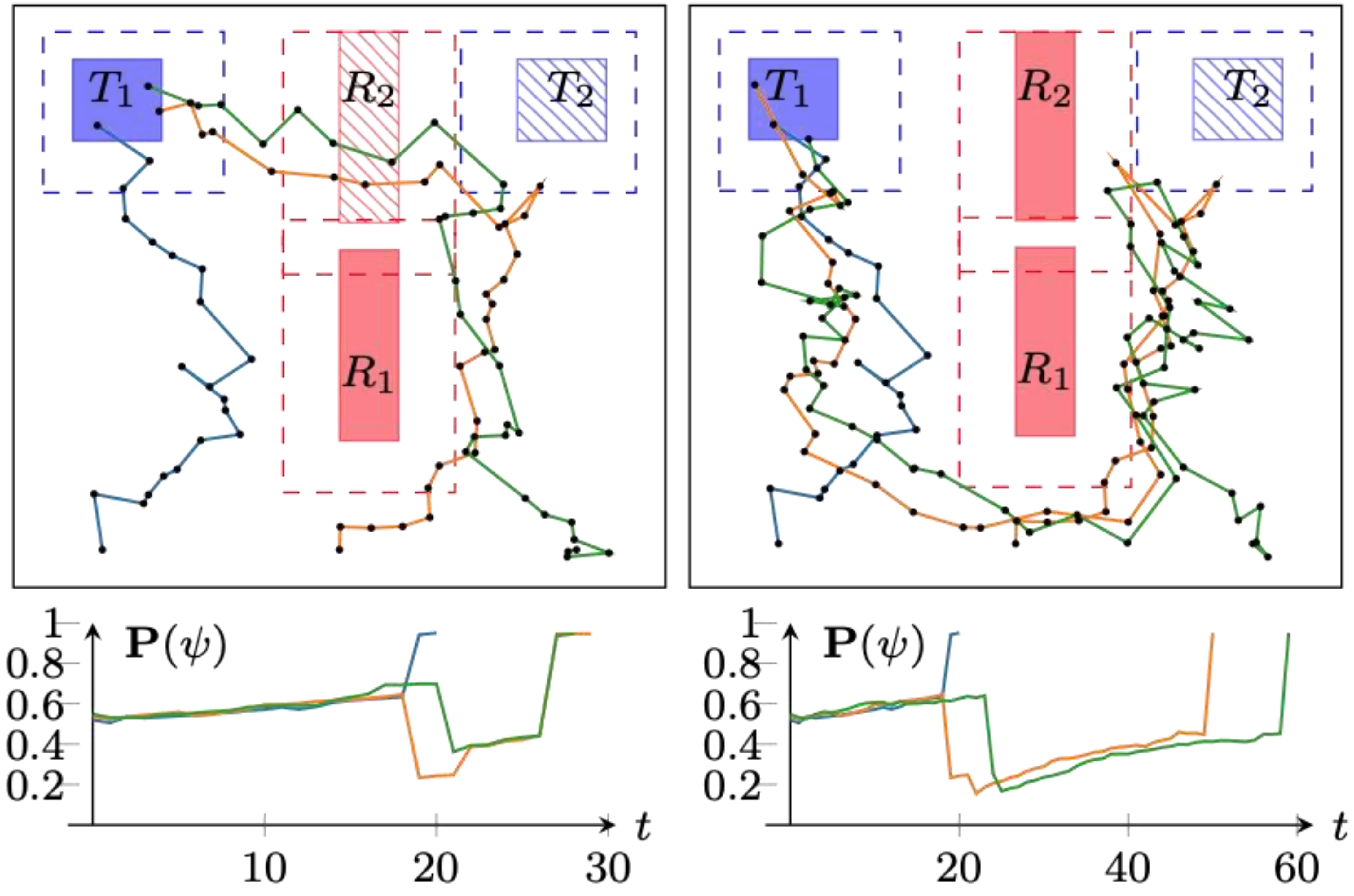
Dealing with partial & noisy observations

How to design and verify digital control?



Computations on abstract model
- Value iterations
- Robust temporal logic satisfaction

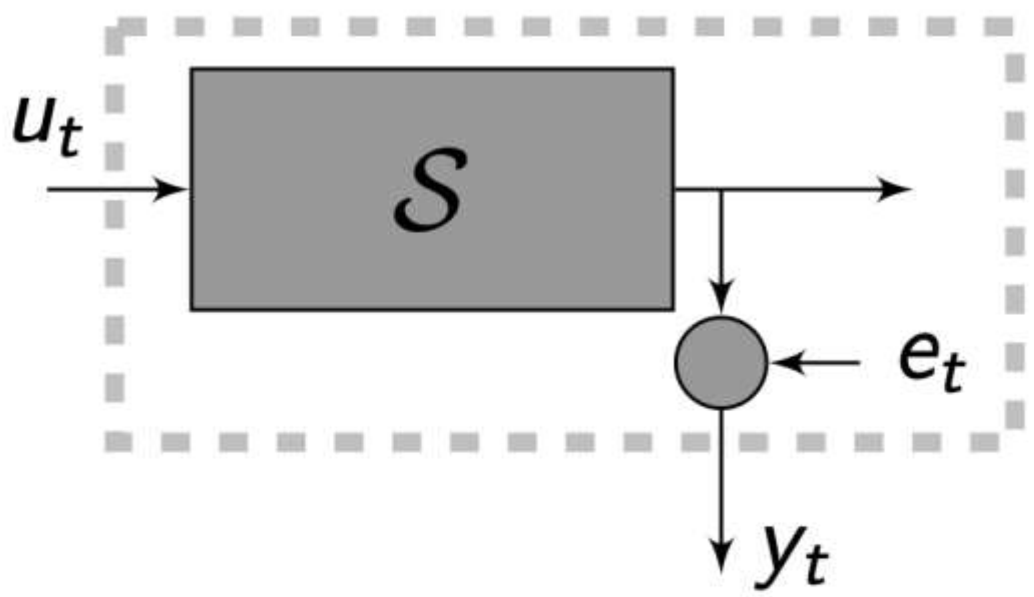
Control refinement to gMDP
- Preserves guarantees



Dealing with model uncertainty in CPS

How to verify functionality using data?

Partially unknown system



$$\left.\begin{aligned} x_{t+1} &= f(x_t, u_t; \theta) + v_t \\ y_t &= h(x_t; \theta) + e_t \end{aligned}\right\} \ \mathbf{M}(\theta) \text{ Parameterized model}$$

θ = unknown parameter

Solution: Use prior knowledge and data

Compute confidence with Bayesian inference

$$\mathbf{P}\left\{\mathbf{M}(\theta) \vDash \psi \mid (u, y)_t\right\}$$

Data obtained from system

S. Haesaert et al. ACC15, CDC15, Automatica17

Dealing with model uncertainty in CPS

How to collect the right data efficiently?

Design experiment input
to gain information on
property satisfaction.

$$\mathbf{P}\big(\mathbf{M}(\theta) \vDash \psi \,|\, \{u, y\}_t\big)$$

Data from experiment

= Optimal control problem

Maximize probability of reaching decision

$$\mathbf{P}\big(\mathbf{M}(\theta) \vDash \psi \,|\, \{u, y\}_t\big) \geq 1 - \delta = \textbf{ accept}$$
$$\mathbf{P}\big(\mathbf{M}(\theta) \vDash \psi \,|\, \{u, y\}_t\big) \leq \delta = \textbf{ reject}$$

Some data is expensive

S. Haesaert et al. ACC15,ECC16

Dealing with uncertainty in safety-critical cyber-physical systems

A control engineering perspective

dr. ir. Sofie Haesaert
Assistant Professor
TU Eindhoven
The Netherlands

Contact me at
Sofiehaesaert.com
s.haesaert@tue.nl

Thank you for your attention

TU/e