ROBOTICS SCIENCE AND SYSTEMS 2021

amazon

TOYOTA RESEARCH INSTITUTE

KTH ROYAL INSTITUTE OF TECHNOLOGY

Formal methods for robot planning

Jana Tumova

Associate Professor

Division of Robotics, Perception and Learning

Why formal methods?

Rigorous techniques for

specification → How do we tell robots what to do?

development, verification, analysis of systems → How do we ensure that they behave as expected?

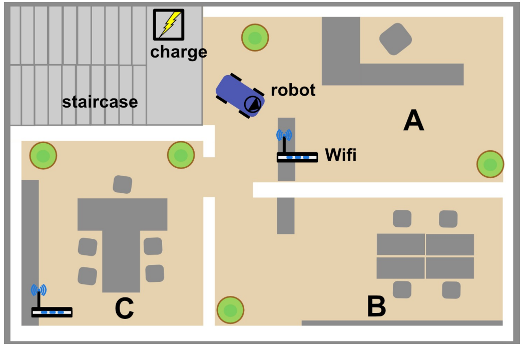
Why temporal logics and formal synthesis?

Temporal logics → How do we tell robots what to do?

- rich
- rigorous
- resemblance to natural language

Formal synthesis → How do we ensure that they behave as expected?

Temporal logic for mission and motion objectives



- Keep patrolling the three offices.

$$GF(A) \wedge GF(B) \wedge GF(C)$$

- Whenever you spot danger, go directly to the staircase and wait for “all clear” signal before continuing.

$$G(danger \Rightarrow X(staircase\ U\ all\_clear))$$

- Make sure to recharge at least every 10 minutes.

$$GF_{[0,10]}recharge$$

- At all times, stay within 5 meters from the wi-fi router.

$$G(Dist(robot, router) \leq 5)$$

Why temporal logics and formal synthesis?

Temporal logics
- rich
- rigorous
- resemblance to natural language

→ How do we tell robots what to do?

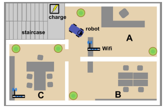
Formal synthesis
- correct-by-design plan

→ How do we ensure that they behave as expected?

KTH VETENSKAP OCH KONST

Formal synthesis

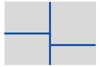
System



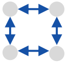
Objective

Patrol offices A and B.

Model $\dot{p}(t) = u(t)$



Abstraction



$GF(A) \wedge GF(B)$ Temporal logic specification

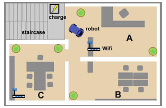
Formal synthesis

A correct-by-design plan

There is no correct-by-design plan

Formal synthesis (2009)

System



Objective

Patrol offices A and B.

Model

Abstraction

DTS, NTS, Petri nets

Temporal logic specification

LTL, GR(1)

Formal synthesis

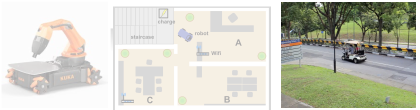
A correct-by-design plan

There is no correct-by-design plan

Some seminal works:
[Kress-Gazit et al, TRO 2009, Kloetzer and Belta, TAC 2008]

Formal synthesis (2013)

System



multi-agent,
partially unknown and
dynamic environments,…

Objective

temporal goals,
additional optimization criteria, deadlines

Model

Non-linear, with disturbance,…

Abstraction

DTS, NTS, Petri nets, roadmaps, trees, WTS, MDPs,…

User-friendly interface

Linguistic, graphical

Temporal logic specification

LTL, GR(1), sc-LTL, PCTL, MTL,…

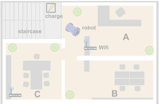
Formal synthesis

A correct-by-design plan

There is no correct-by-design plan

Formal synthesis (today)

System


multi-agent,
partially unknown and
dynamic environments,…

Model

Non-linear, with disturbance,…

Abstraction

DTS, NTS, Petri nets, roadmaps, trees, WTS, MDPs,…

Objective

temporal goals,
additional optimization criteria, deadlines
spatio-temporal goals and constraints,…

User-friendly interface

Linguistic, graphical

Temporal logic specification

LTL, GR(1), sc-LTL, PCTL, MTL, STL,…

Formal synthesis

A correct-by-design plan

There is no correct-by-design plan

Formal synthesis, integrated

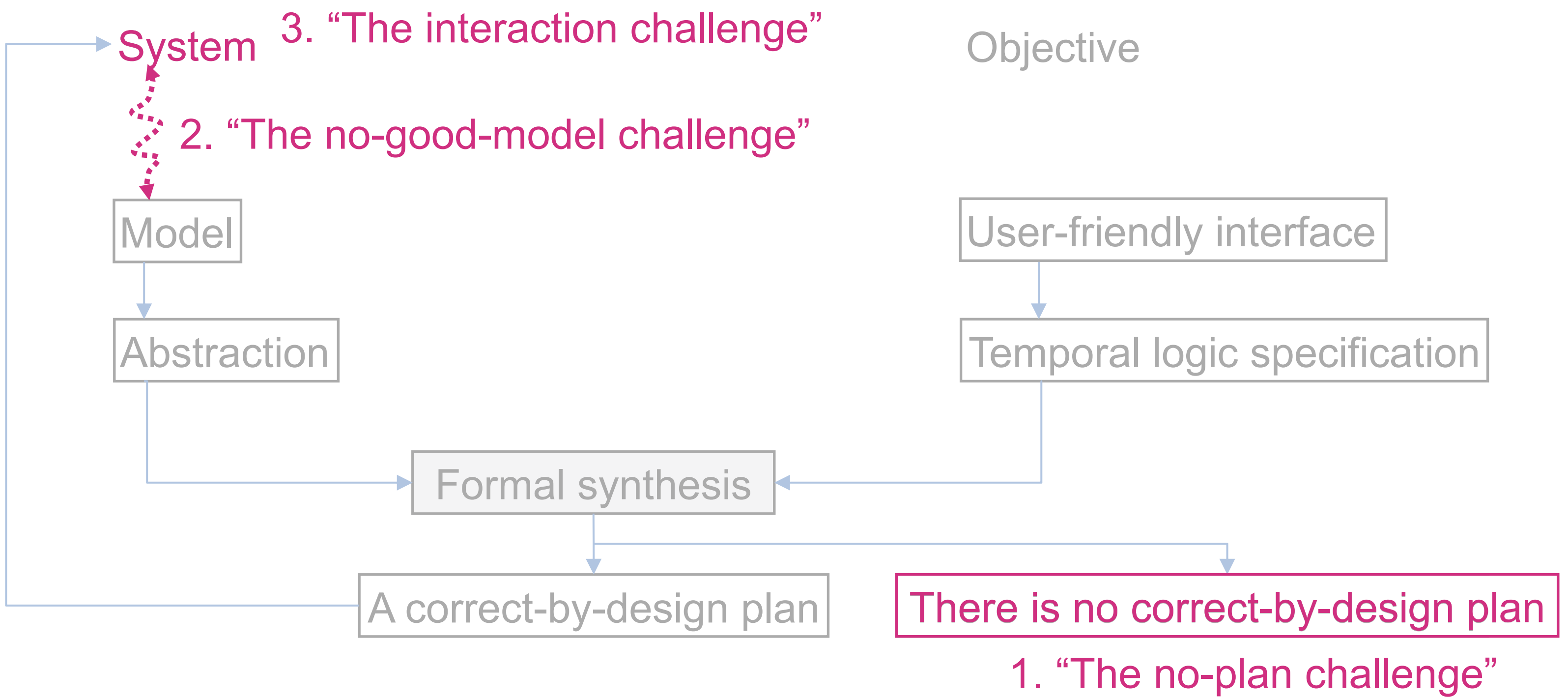
4Robots

Multi-robot coordination
for dynamic production assistance

KTH VETENSKAP OCH KONST · BOSCH Invented for life · National Technical University of Athens · PAL ROBOTICS · FORTH Foundation for Research & Technology

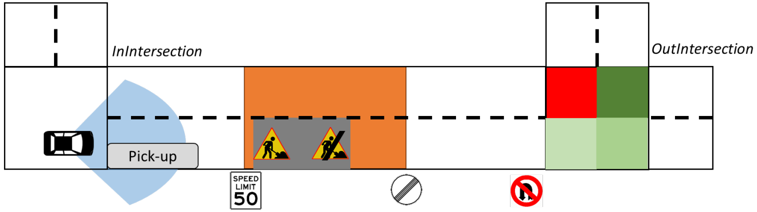
www.co4robots.eu

Three challenges of formal synthesis



1. The no-plan challenge

System



Objective

Obey the traffic rules:

- Do not cross the full lane
- Stay in the right lane
- Do not enter the construction zone
- Do not enter sidewalk

…

Model, abstraction

Temporal logic specification

LTL over finite traces

Formal synthesis

A correct-by-design plan

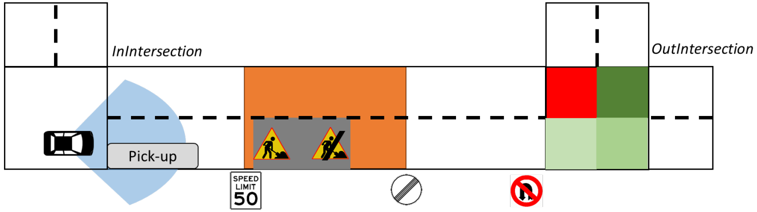
There is no correct-by-design plan

All the traffic rules cannot be obeyed simultaneously

KTH VETENSKAP OCH KONST

1. The no-plan challenge

System



Model, abstraction

Objective

Obey the traffic rules:

- Do not cross the full lane
- Stay in the right lane
- Do not enter the construction zone
- Do not enter sidewalk

…

Temporal logic specification

LTL over finite traces

Formal synthesis

A plan as correct as possible

The traffic rules are violated only for the absolutely necessary, for the necessary time

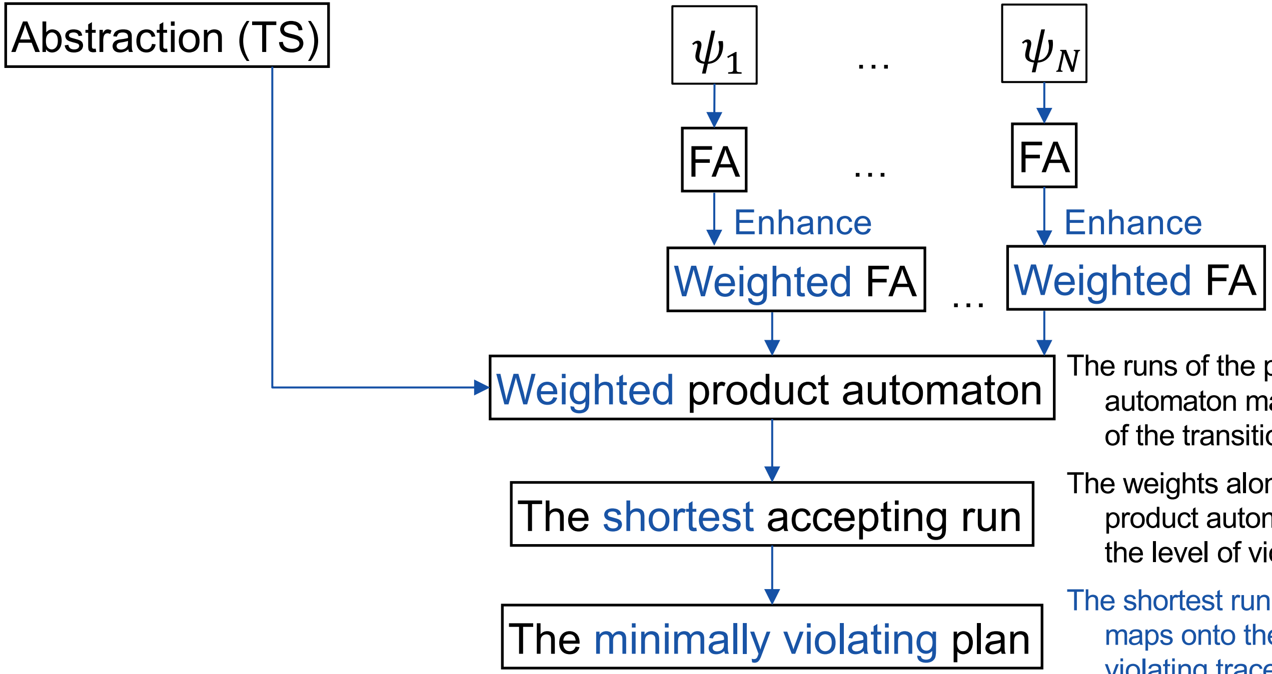
Quantitative evaluation of LTL

Assume a transition system from RRT* or other abstraction

Level of violation $\lambda(trace, LTL\ formula)$**:** the time duration associated with the discrete transitions that need to be removed to make the trace satisfy the LTL formula, weighted by the penalty

[Tumova et al HSCC 2013]

Minimum-violation automata-based FS



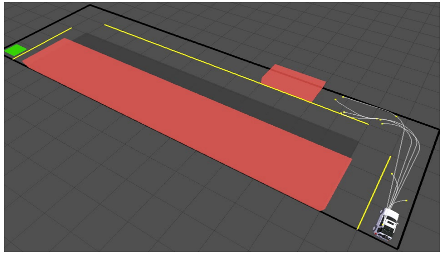
- The runs of the product automaton map to the traces of the transition system
- The weights along the run of the product automaton determine the level of violation
- The shortest run of the product maps onto the minimally violating trace of the model

[Tumova et al HSCC 2013]

KTH VETENSKAP OCH KONST

MV-RRT*

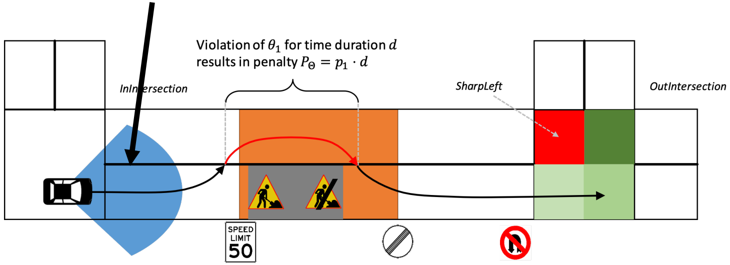
	RRT*	MV-RRT*
• Incrementally build	weighted tree	weighted product automaton
• Incrementally update	shortest path	minimally violating path
• Optimality criterion	distance	primarily level of violation, then distance



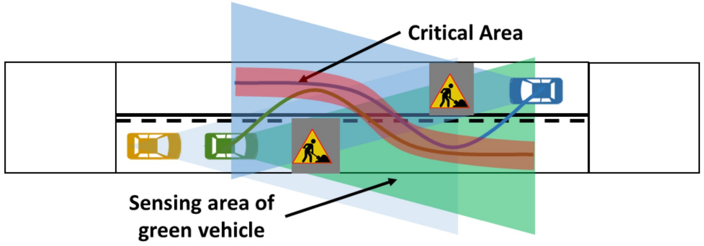
[Reyes-Castro et al CDC 2013]

MV-RRT* in autonomous driving

Limited sensing:



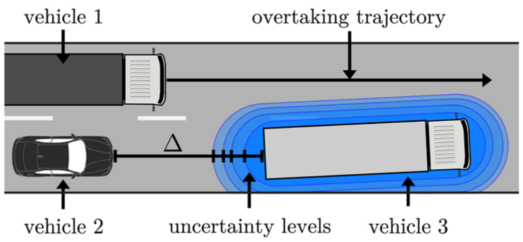
Multi-vehicle settings:



[Reyes-Castro et al HSCC 2013, Vasile et al ICRA 2017, Karlsson et al ICRA 2018, CASE 2020, ICRA 2021]

The no plan challenge under uncertainty

System



Model, abstraction

Objective

Common sense/RSS:

- Keep a safe distance $\Delta(v_e, v_l)$
- …

Temporal logic specification

STL

$G(\Delta(v_e, v_l) - (p_l - p_e) > 0)$

Formal synthesis

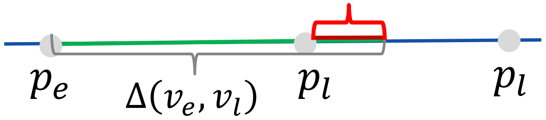
A plan as correct as possible

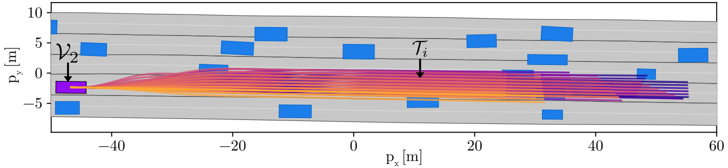
The severity of violation, the probability of violation, and the level of uncertainty are taken into account

Risk-aware planning in autonomous driving

- Safety specification: $G\big(h(x(t)) > 0\big)$
- Severity function: $\ell_h(x) = \begin{cases} \ell\big(h(x(t))\big), h(x(t)) > 0 \\ 0, \text{otherwise} \end{cases}$
- Severity of violation: $L = l_h(\hat{x})$
- Risk: $E[L]$
- Risk-aware planning

$G(\Delta(v_e, v_l) - (p_l - p_e) > 0)$





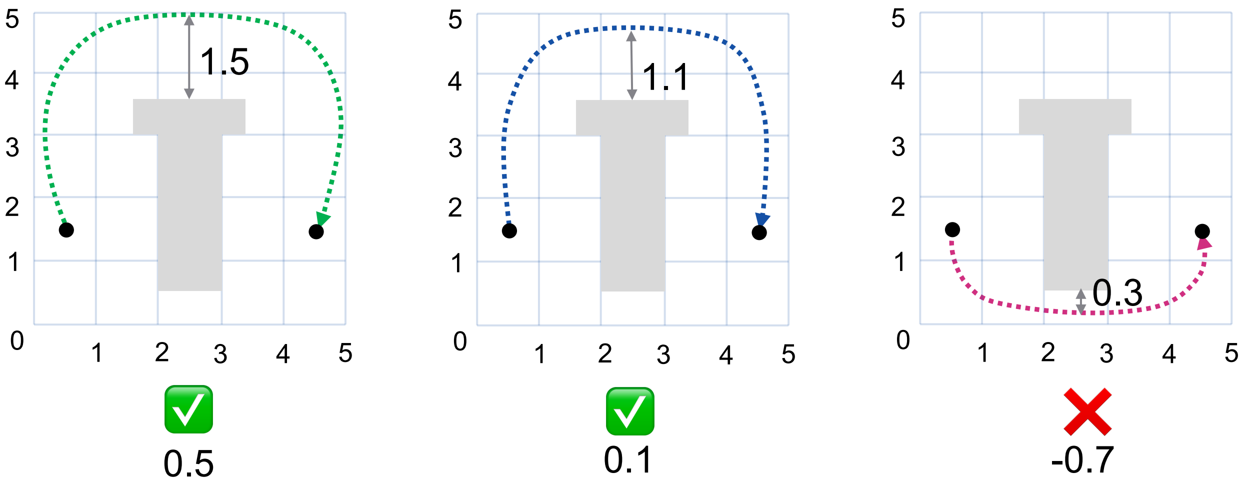
US101 highway scenario

[Nyberg et al IV 2021]

KTH VETENSKAP OCH KONST

Signal Temporal Logic spatial robustness

$$G(1 - dist(\sigma, M) > 0)$$



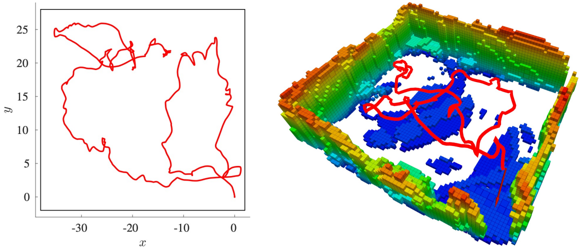
See [Donze and Maler, LNCS, 2013]

KTH VETENSKAP OCH KONST

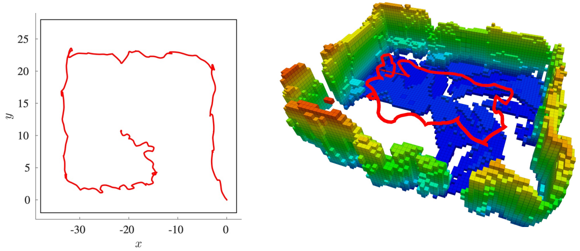
STL as a preference specification

STL-guided autonomous exploration

AEP



AEP + STL $G(dist(\sigma, M) - 1 > 0)$



Guiding Autonomous Exploration with Signal Temporal Logic

Fernando S. Barbosa, Daniel Duberg, Patric Jensfelt and Jana Tumova

[Barbosa et al RA-L 2019]

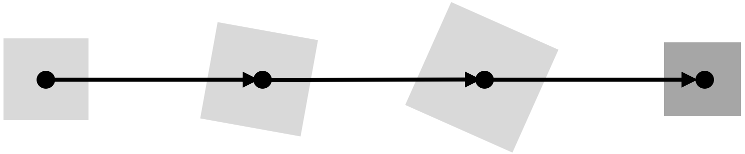
2. The no-good-model challenge

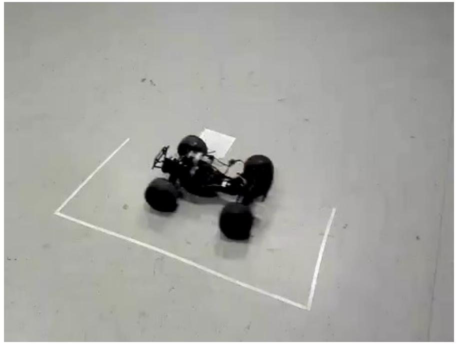
KTH VETENSKAP OCH KONST

Safe multi-step feedback motion primitives

for non-holonomic system with bounded disturbance

- Divide the input space into regions & linearize
- Linearization introduces error





- The error can be corrected in *k* steps
- The motion primitives can be chained and refined

[Tajvar et al ISSR 2019, CASE 2020, IROS 2021]

LTL planning with motion primitives

System

Objective

LTL specification

BA

Motion primitives

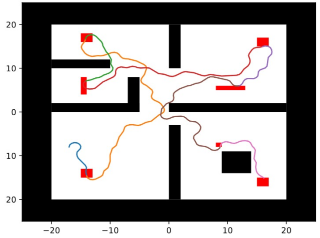
Backward reachability tree

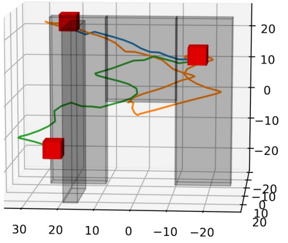
heuristics

Modified A*

refine

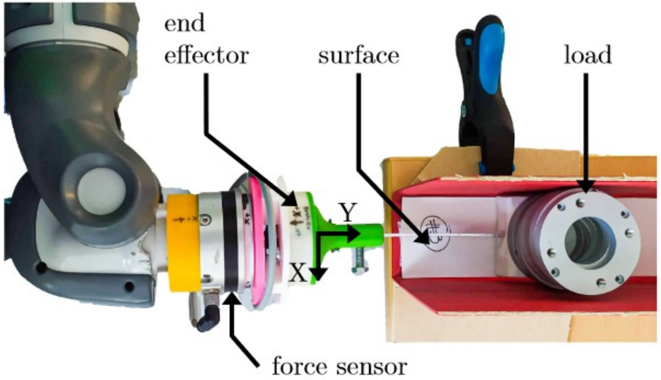
A correct-by-design plan

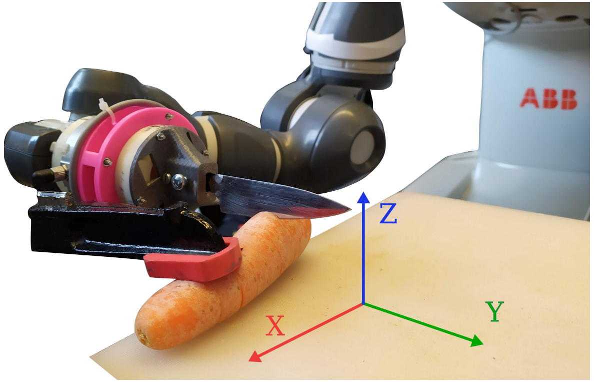




[Tajvar et al CASE 2020]

Towards safe data-driven contact-rich manipulation





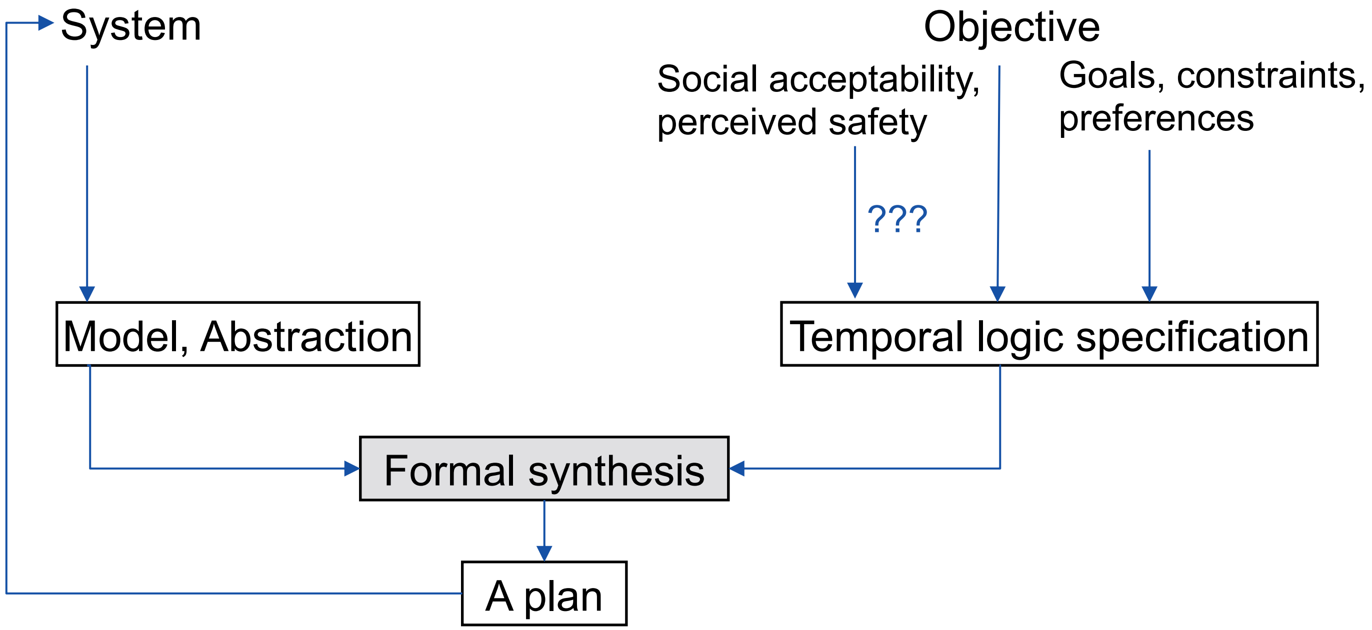
[Mitsioni et al Humanoids 2021]

KTH VETENSKAP OCH KONST

The social interaction challenge

KTH VETENSKAP OCH KONST

Correct-by-design and socially acceptable plan

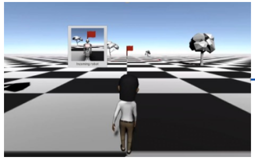


KTH VETENSKAP OCH KONST

Correct-by-design and socially acceptable plan

System

Interactions



inference

Objective

Social acceptability, perceived safety

Goals, constraints, preferences

STL with probabilistic predicates

Model, Abstraction

Temporal logic specification

Formal synthesis

A plan

Linard et al CASE 2020, IROS 2021

KTH VETENSKAP OCH KONST

I wish I had time to talk also about

- Provable safety vs. perceived safety
- Assumption-guarantee synthesis

- Decentralized multi-agent coordination with temporal logic specifications

KTH VETENSKAP OCH KONST

Take-aways

- Temporal logics and formal synthesis to address
  - How do we tell robots what to do?
  - How do we ensure that they behave as expected?
- Rigorous, **but not rigid**:
  - Can be used to provide guarantees if that is desired and possible
  - No need to freeze if a correct-by-design plan does not exist
  - Support for preferences, not just mission/safety-critical goals

The future: Moving forward to the wild

- Well-defined mathematical objectives → "Soft" objectives
- Guarantees → Risk-awareness
- Manually created models and specifications → Data-driven models and specifications
- FS or learning → FS and learning

  RL with TL goals, RL with TL constraints,
- Component-view → System-view

KTH VETENSKAP OCH KONST

Thanks!

Pouria Tajvar, Truls Nyberg, Fernando Barbosa, Wei Wang, Albin Larsson Forsberg, Georg Schuppe, Alexis Linard, Christian Pek, Jesper Karlsson

Swedish Research Council

Horizon2020 European Union Funding for Research & Innovation

Swedish Foundation for Strategic Research

WASP Wallenberg Autonomous Systems and Software Program

digital futures

VINNOVA Sweden's Innovation Agency