Logical Verification and Systematic Parametric Analysis in Train Control

André Platzer and Jan-David Quesel

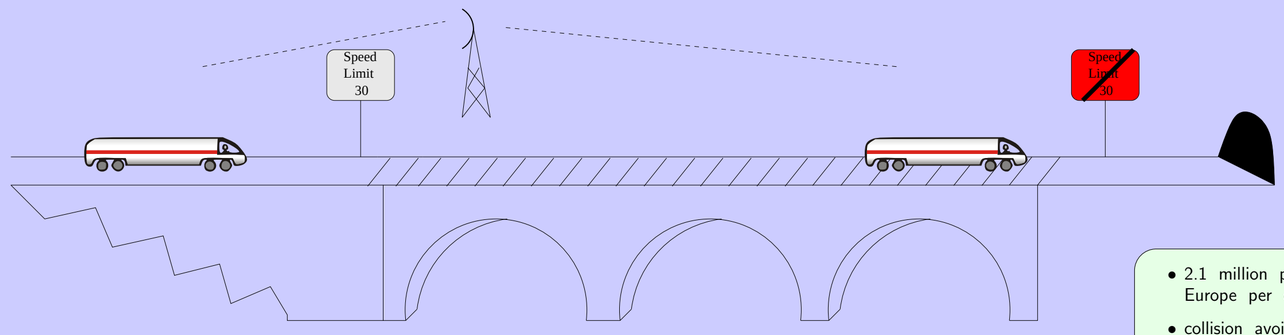
University of Oldenburg

Correct System Design
University of Oldenburg

Abstract

We formally verify hybrid safety properties of cooperation protocols in a fully parametric version of the *European Train Control System* (ETCS). We present a formal model using hybrid programs and verify correctness using our logic-based decomposition procedure. This procedure supports free parameters and parameter discovery, which is required to determine correct design choices for free parameters of ETCS.

Keywords: parametric verification, logic for hybrid systems, symbolic decomposition



- 2.1 million passengers in Europe per day
- collision avoidance
- maximize throughput
- speed up to 300 km/h

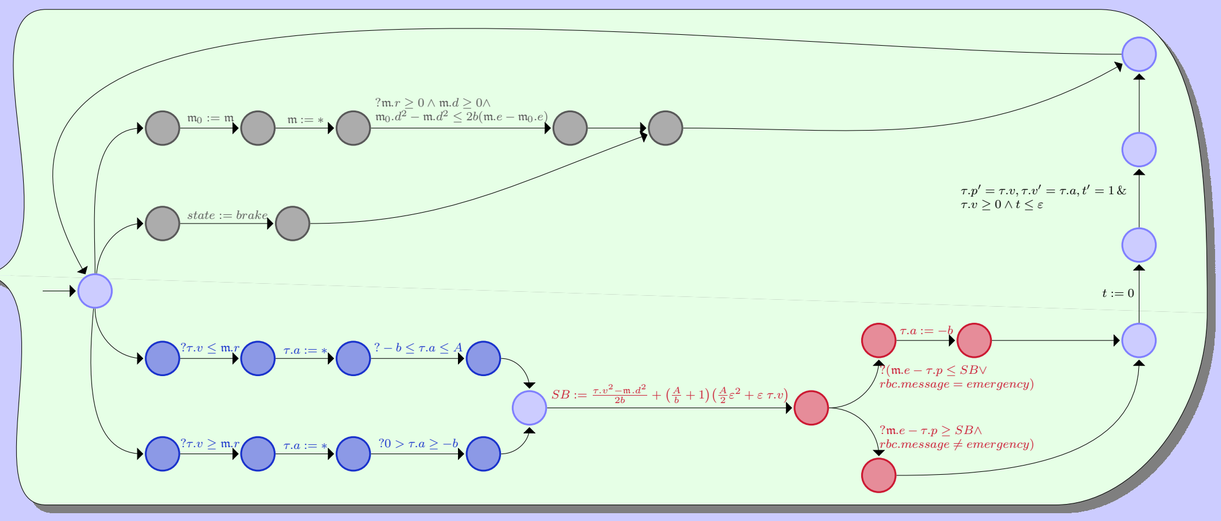
Differential Dynamic Logic dℒ

$\phi ::= \theta_1 \sim \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x\phi \mid \exists x\phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$

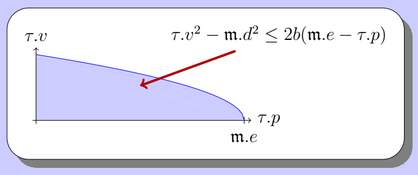
Hybrid Program	Effect
$\alpha;\ \beta$	sequential composition
$\alpha\ \cup\ \beta$	nondeterministic choice
α^*	nondeterministic repetition
$x := \theta$	discrete jump
$x := *$	nondeterministic assignment
$(x_1' = \theta_1, \ldots, x_n' = \theta_n, F)$	continuous evolution of x_i along $x_i' = \theta_i$, restricted to region F
$?F$	check if F holds at current state

European Train Control System (ETCS)

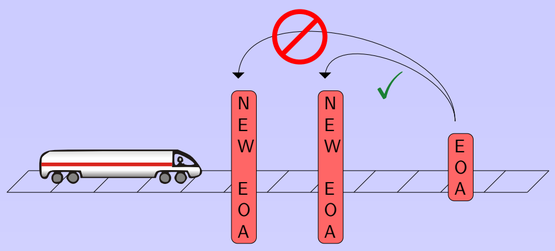
ETCS : (train ∪ rbc)*
train : spd; atp; move
spd : $(?\tau.v \le \mathrm{m}.r;\ \tau.a := *;\ ?-b \le \tau.a \le A)$
$\cup(?\tau.v \ge \mathrm{m}.r;\ \tau.a := *;\ ?0 > \tau.a \ge -b)$
atp : $SB := \frac{\tau.v^2 - \mathrm{m}.d^2}{2b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon\,\tau.v\right)$;
$(?(\mathrm{m}.e - \tau.p \le SB \vee rbc.message = emergency);\ \tau.a := -b)$
$\cup(?\mathrm{m}.e - \tau.p \ge SB \wedge rbc.message \ne emergency)$
move : $t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \,\&\, \tau.v \ge 0 \wedge t \le \varepsilon)$
rbc : $(rbc.message := emergency)$
$\cup\ (\mathrm{m}_0 := \mathrm{m}; \mathrm{m} := *;\ ?\mathrm{m}.r \ge 0 \wedge \mathrm{m}.d \ge 0 \wedge \mathrm{m}_0.d^2 - \mathrm{m}.d^2 \le 2b(\mathrm{m}.e - \mathrm{m}_0.e))$



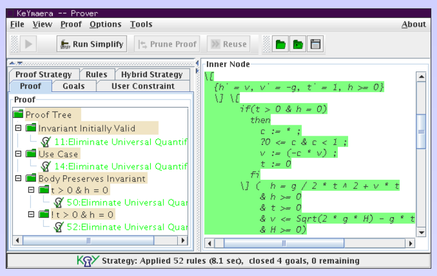
Controllability

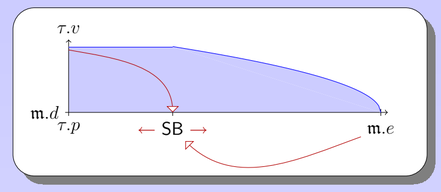


$[\tau.p' = \tau.v, \tau.v' = -b \,\&\, \tau.v \ge 0](\tau.p \ge \mathrm{m}.e \rightarrow \tau.v \le \mathrm{m}.d)$
$\equiv \tau.v^2 - \mathrm{m}.d^2 \le 2b(\mathrm{m}.e - \tau.p)$



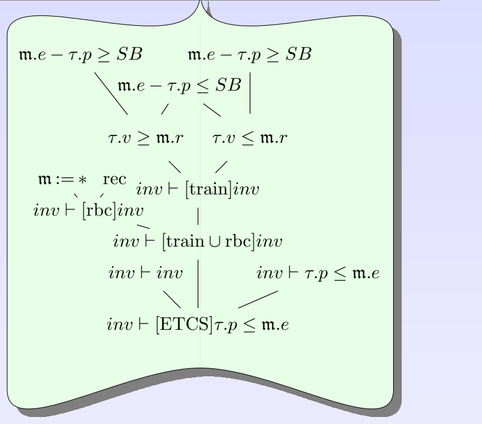
$\forall\tau\Big((\tau.v^2 - \mathrm{m}.d^2 \le 2b(\mathrm{m}.e - \tau.p) \wedge \tau.v \ge 0 \wedge \mathrm{m}.d \ge 0 \wedge \varepsilon > 0)$
$\rightarrow [\mathrm{m}_0 := \mathrm{m};\ rbc]\ (\mathrm{m}_0.d^2 - \mathrm{m}.d^2 \le 2b(\mathrm{m}.e - \mathrm{m}_0.e)$
$\rightarrow \tau.v^2 - \mathrm{m}.d^2 \le 2b(\mathrm{m}.e - \tau.p))\Big)$

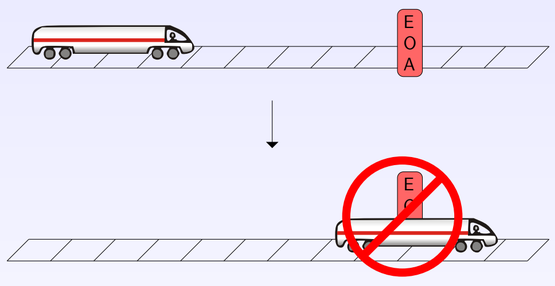




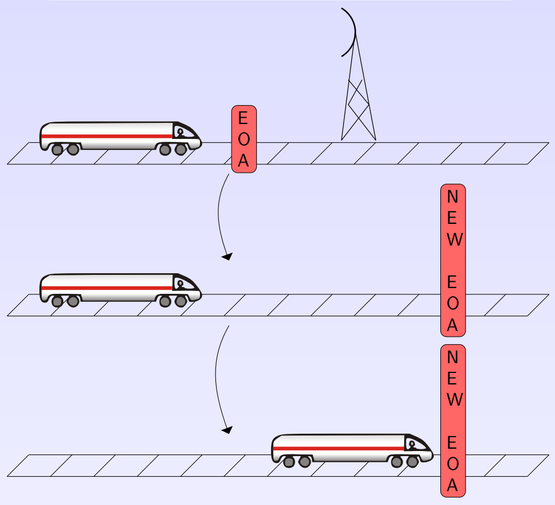
$(\tau.v^2 - \mathrm{m}.d^2 \le 2b(\mathrm{m}.e - \tau.p) \wedge \tau.v \ge 0 \wedge \mathrm{m}.d \ge 0 \wedge \varepsilon > 0)$
$\rightarrow [\mathrm{m}_0 := \mathrm{m};\ rbc](\mathrm{m}_0.d^2 - \mathrm{m}.d^2 \le 2b(\mathrm{m}.e - \mathrm{m}_0.e)$
$\rightarrow [spd]\langle SB := *\rangle[atp;\ move](\tau.p \ge \mathrm{m}.e \rightarrow \tau.v \le \mathrm{m}.d))$

$(\tau.v^2 - \mathrm{m}.d^2 \le 2b(\mathrm{m}.e - \tau.p) \wedge \tau.v \ge 0 \wedge \mathrm{m}.d \ge 0 \wedge \varepsilon > 0)$
$\rightarrow [\mathrm{ETCS}](\tau.p \ge \mathrm{m}.e \rightarrow \tau.v \le \mathrm{m}.d)$





$(\tau.v^2 - \mathrm{m}.d^2 \le 2b(\mathrm{m}.e - \tau.p) \wedge \mathrm{m}.d \ge 0 \wedge \varepsilon > 0) \wedge \tau.v > 0$
$\rightarrow \forall P\ \langle \mathrm{ETCS} \rangle\ \tau.p \ge P$



RBC Controllability

Reactivity

Safety

Liveness

References

[1] Damm, W., Hungar, H., Olderog, E.R.: Verification of cooperating travel agents. International Journal of Control **79**(5) (May 2006) 395–421

[2] ERTMS User Group, UNISIG: ERTMS/ETCS System requirements specification (2002) Version 2.2.2.

[3] Platzer, A.: Differential dynamic logic for verifying parametric hybrid systems. In Olivetti, N., ed.: TABLEAUX. Volume 4548 of LNCS., Springer (2007) 216–232

[4] Platzer, A.: Differential dynamic logic for hybrid systems. J. Autom. Reasoning (2008)

Deutsche Forschungsgemeinschaft DFG

CARL VON OSSIETZKY universität OLDENBURG

ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

UNIVERSITÄT DES SAARLANDES