RAILCONS

Design-time capacity – SAT modulo Discrete Event Simulation

RailCOMPLETE   UiO : University of Oslo

Capacity

This work addresses a central problem that occurs when designing the layout and control systems for railway stations: Does the station infrastructure have the *capacity* to handle the amount of trains and the desired traveling times?

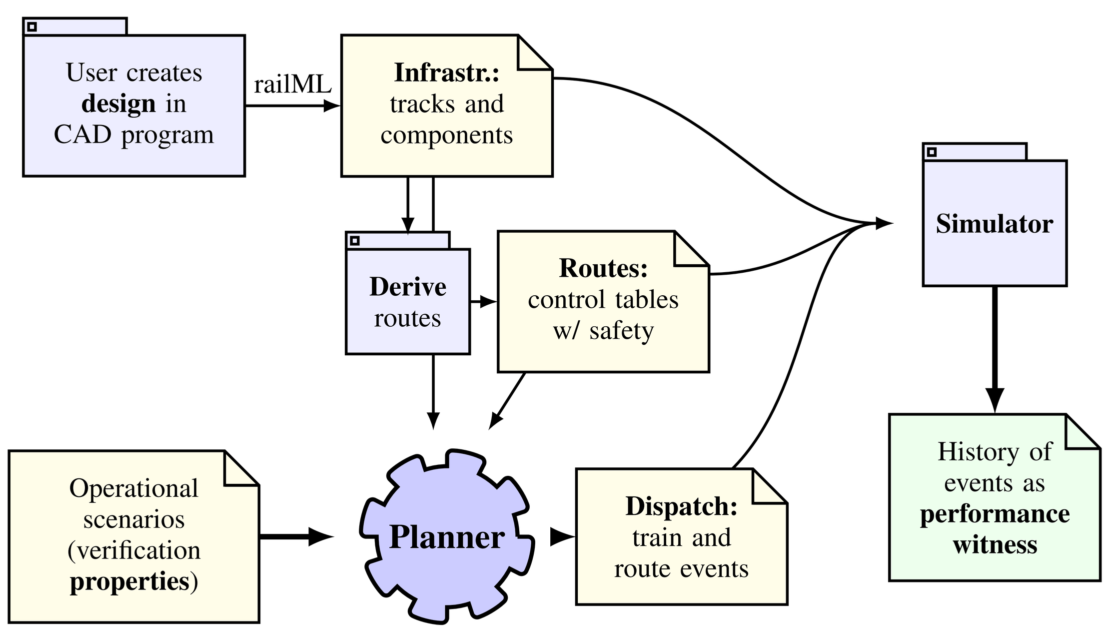
We consider **the low-level railway infrastructure capacity verification problem**, defined as follows:

> Given a railway station track plan including signaling components, rolling stock dynamic characteristics, and a performance/capacity specification, verify whether the specification can be satisfied and find a dispatch plan as a witness to prove it.

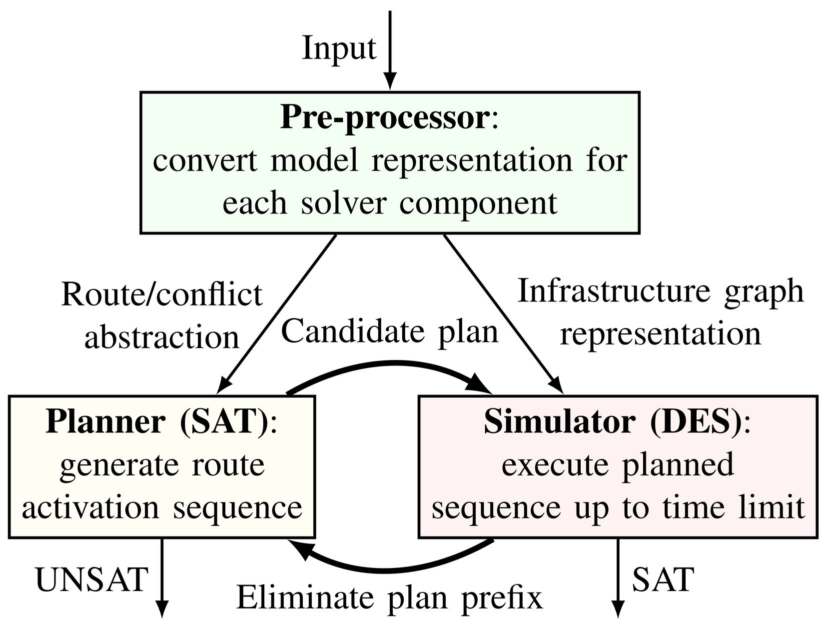
Solving this problem subsumes the following railway infrastructure design activities:

- Low-level **running time** analysis – verify the time required for getting from point A to point B.
- Low-level **schedulability** analysis – verify frequency of trains arriving at a station, and simultaneous opportunities for crossing, parking, loading, etc.
- **Combinations** – verify running time requirements on schedulable operations.

Solver architecture

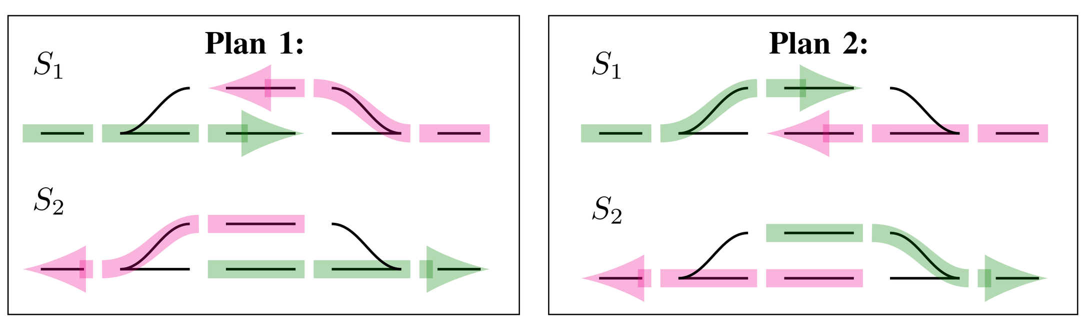


The planner part of the tool chain is implemented in a CEGAR loop:



Synthesis / optimization

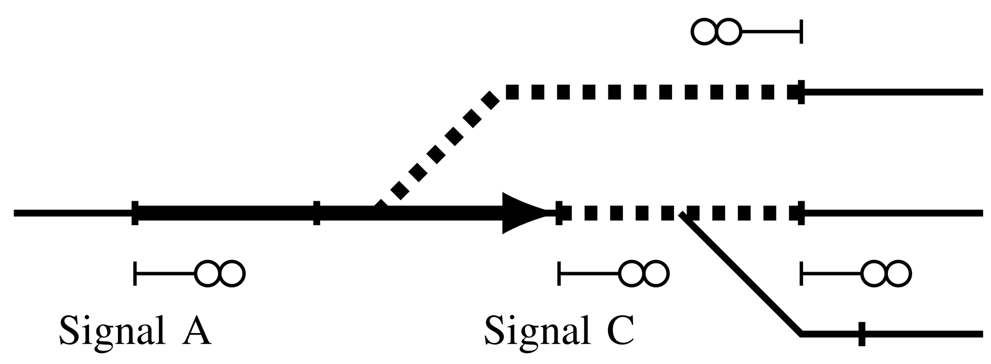
1. **Redundancy:** The planner can be used to detect whether some equipment in the design is redundant. If a plan can be found which does require any use of certain pieces of signalling equipment, these pieces can be considered for removal from the design.
2. **Maximal design:** we can find all relevant locations to place signals (maximum *schedulability*) by placing signals near every switch/branch, turning the signal placement synthesis problem into optimization.
3. **Running time optimization:** starting from a design schedulable which satisfies schedulability requirements, signals placement can be adjusted locally to achieve timing constraints.



Constraints

Physical infrastructure

Trains travel on a network of railway tracks which have **(1) physical properties** such as length, gradient, curvature, etc., **(2) topology** determined by the location of switches (branches), **(3) equipment** such as signals and detectors, and **(4) sight** information showing from which parts of tracks a signal is visible.



Communication constraints

After movement has been allowed by the control system, the driver must be informed of this fact.

- Communication is limited by how many different aspects the lamps can show. To avoid high-speed trains slowing down at every signal, several consecutive elementary routes can be signaled in advance using so-called distant signals.
- Automatic train protection systems (ATP)
- European Rail Traffic Management System (ERTMS) uses long-range radio for communication, effectively removing the communication constraint.

Allocation of resources

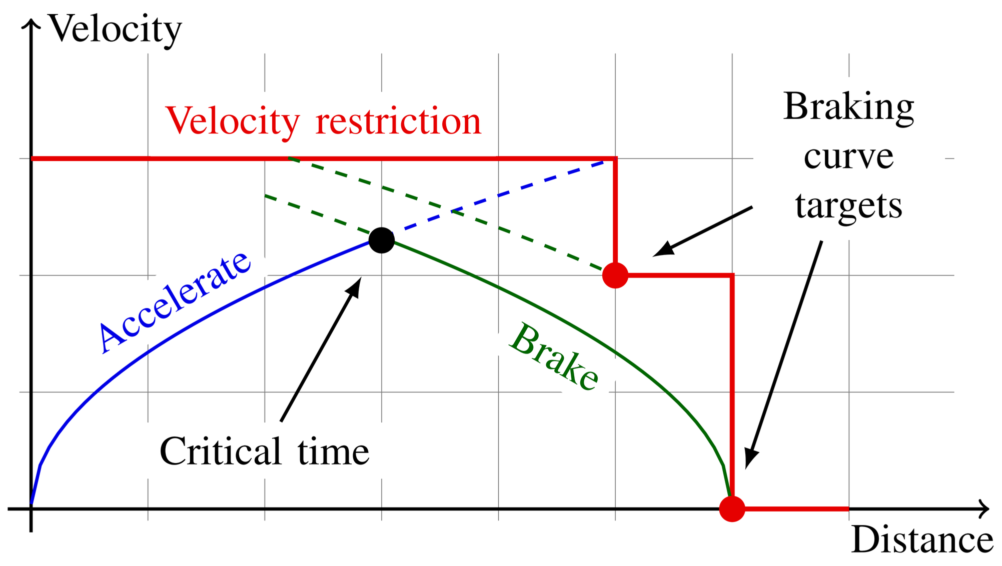
Avoiding collisions by exclusive use of resources is the responsibility of the interlocking, which takes requests from the dispatcher for activating **elementary routes**.

1. **Wait for resources**: track segments and switches in the route path must be free.
2. **Movable elements**: set switches into position.
3. **Signals**: show proceed aspect until train has passed.
4. **Release**: wait for the train to leave, then deallocate.

Laws of motion

Trains move according to the laws of motion, accelerating towards the current maximum speed, while also braking in time to meet all speed restrictions ahead v_i:

$$v - v_0 \leq a\Delta t \qquad v^2 - v_i^2 \leq 2bs_i$$



Specifications

Operational scenario

To capture typical performance and capacity requirements in construction projects, we define an **operational scenario** $S = (V, M, C)$ as follows:

1. A set of **vehicle types** V, each defined by a length l, a maximum velocity $v_{\max}$, a maximum acceleration a, and a maximum braking retardation b.
2. A set of **movements** M, each defined by a vehicle type and an ordered sequence of visits. Each visit q is a set of alternative locations $\{l_i\}$ and an optional minimum dwelling time t_d.
3. A set of **timing constraints** C, which are two visits q_a, q_b, and an optional numerical constraint t_c on the minimum time between visit q_a and q_b. The two visits can come from different movements. If the time constraint t_c is omitted, the visits are only required to be ordered, so that $t_{q_a} < t_{q_b}$.

Running time

An expectation of how long it should take for a train to travel between two locations.

```
movement passengertrain {
  visit #a [b1]; visit #b [b2] }
timing a <90.0 b
```

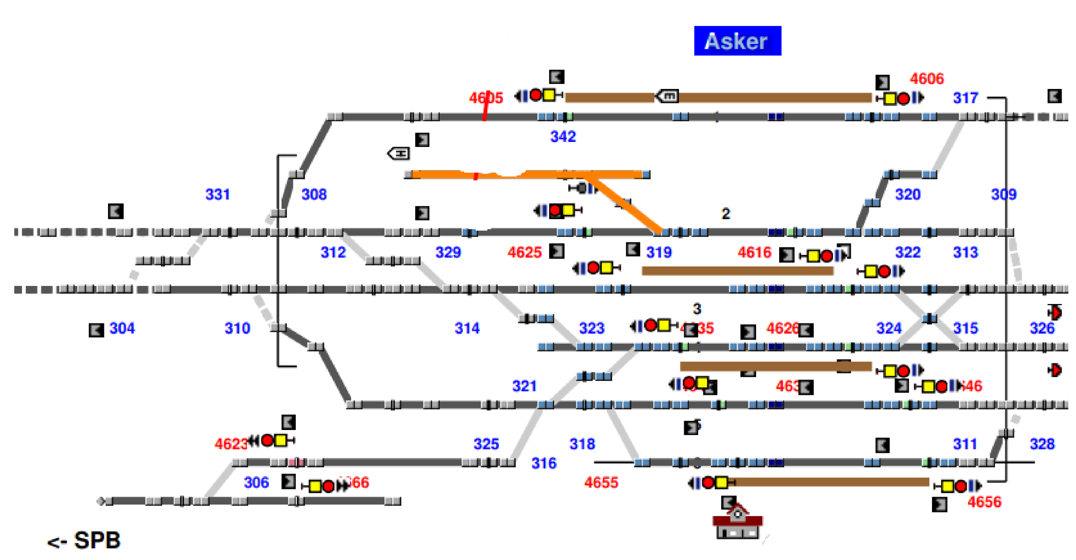
Crossing

Trains traveling in *opposite directions* can visit a station simultaneously.

```
movement passengertrain {
  visit #p_in [b1]; visit #p_out [b2] }
movement goodstrain {
  visit #g_in [b2]; visit #g_out [b1] }
timing p_in < g_out
timing g_in < p_out
```

Case studies

Infrastructure



Source: Bane NOR SF, Norway.

Case studies were performed using:

1. an infrastructure model from the Arna construction project made using the RailCOMPLETE® railway signalling CAD software.
2. the Norwegian railway infrastructure manager Bane NOR supplies a railML infrastructure model of the whole national railway network from which we have extracted examples.

Performance table

Infrastructure	Property	Result	n_{DES}	t_{SAT}	t_{DES}	t_{total}
Two track (14 elem.)	Run.time	Sat.	1	0.01	0.00	0.01
	Frequency	Sat.	1	0.01	0.00	0.01
	Overtaking 2	Sat.	1	0.00	0.00	0.01
	Overtaking 3	Unsat.	0	0.01	0.00	0.01
	Crossing 3	Unsat.	0	0.01	0.00	0.01
Kolbotn (BN) (56 elem.)	Run. time	Sat.	2	0.01	0.00	0.02
	Overtake 4	Sat.	1	0.05	0.00	0.06
	Overtake 3	Unsat.	0	0.05	0.00	0.06
Eidsvoll (BN) (64 elem.)	Run. time	Sat.	2	0.01	0.00	0.02
	Overtake 2	Sat.	1	0.08	0.00	0.08
	Crossing 3	Sat.	1	0.04	0.00	0.04
	Crossing 4	Unsat.	0	0.21	0.00	0.21
Asker (BN) (170 elem.)	Overtaking 2	Sat.	1	0.20	0.00	0.21
	Overtaking 3	Unsat.	1	0.73	0.00	0.74
	Crossing 4	Sat.	0	0.75	0.00	0.77
Arna (CAD) (258 elem.)	Run. time	Sat.	1	0.02	0.00	0.04
	Overtaking 2	Sat.	1	0.50	0.00	0.51
	Overtaking 3	Sat.	1	1.43	0.00	1.45
	Crossing 4	Sat.	1	1.73	0.00	1.74
Gen. 3x3 (74 elem.)	High time	Sat.	1	0.01	0.00	0.01
	Low time	Unsat.	27	0.18	0.01	0.19
Gen. 4x4 (196 elem.)	High time	Sat.	1	0.01	0.00	0.03
	Low time	Unsat.	256	2.08	0.26	2.34
Gen. 5x5 (437 elem.)	High time	Sat.	1	0.06	0.00	0.09
	Low time	Unsat.	3125	38.89	4.35	43.24

TABLE I: Verification performance on test cases, including Bane NOR (BN) and RailCOMPLETE (CAD) infrastructure models. The number of elementary routes (*elem.*) indicates the model's size. n_{DES} is the number simulator runs, t_{SAT} the time in seconds spent in SAT solver, t_{DES} the time in seconds spent in DES, and t_{total} the total calculation time in seconds.

Presented at **FMCAD 2018: Formal Methods in Computer-Aided Design** in Austin, Texas, ***Co-author: Koen Claessen***, Chalmers University.