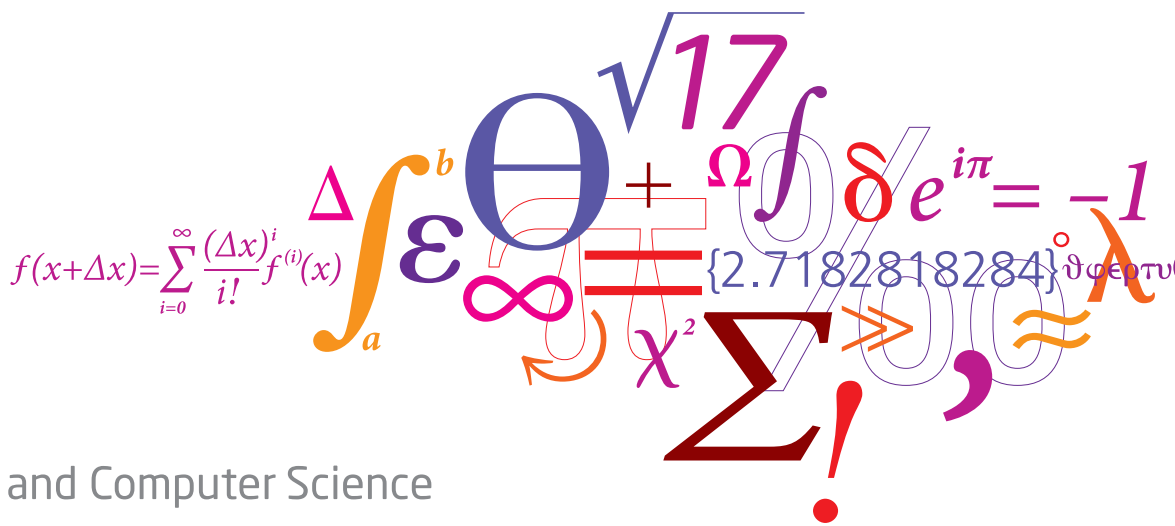
Formel Modellering og Verifikation af Jernbanekontrolsystemer

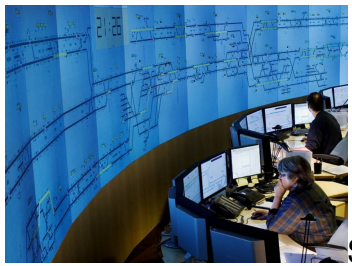
Et eksempel fra RobustRailS WP 4.1

Lektor Anne E. Haxthausen
Railway Verification Group, DTU Compute
Danmarks Teksniske Universitet
(aeha@dtu.dk)



DTU Compute
Department of Applied Mathematics and Computer Science

Forskning

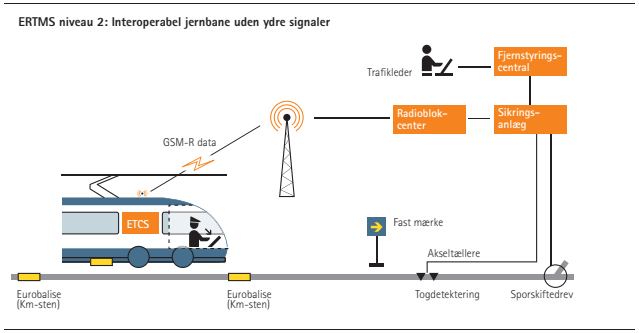

Source: Lisebobek/Banedanmark

- I Railway Verification Group[1] på DTU Compute har vi igennem 20 år forsket i formelle metoder og deres anvendelser til jernbanesystemer (i Danmark og Tyskland).
- Denne præsentation giver et eksempel på dette fra RobustRailS WP 4.1[2]:
  - Vi har udviklet en **formel metode** og et **prototype værktøj** til **automatiseret verifikation** af sikkerhedskritisk software i sikringsanlæg i signalsystemer.

[1] `http://www2.imm.dtu.dk/~aeha/Railway/`

[2] `http://www.imm.dtu.dk/~aeha/RobustRailS/`

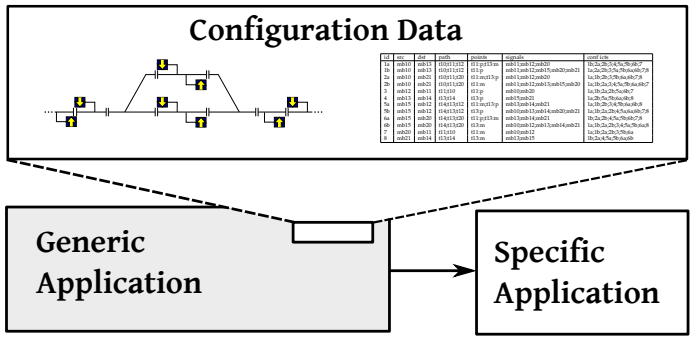
Baggrund



Source: Lisebobek/Banedanmark

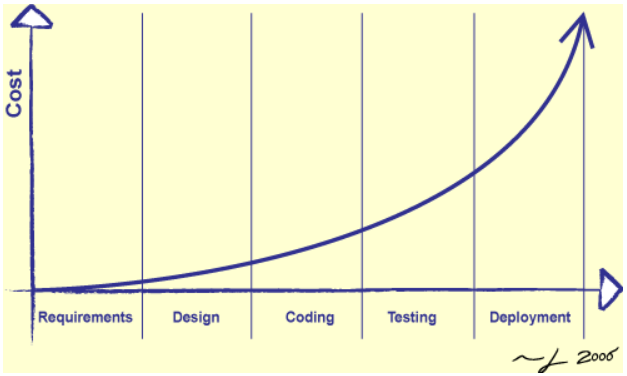
- **Signal Programmet**: nye moderne, computer-baserede signalsystemer.
- Centrale komponenter (f.eks. sikringsanlæggene) af disse er *sikkerhedskritiske*.
- **Udvikling og verifikation** af sådanne systemer
  - er udfordrende
  - gøres konventionelt *manuelt* og *uformelt*
    $\rightarrow$ tidskrævende og med risiko for fejl
  - Der er derfor behov for *automatisering* og *formelle metoder* (jf. CENELEC 50128, som stærkt anbefaler formelle metoder for SIL 3-4 software)
- **Formelle Metoder**: benytter matematisk baserede sprog og teknikker til at specificere og verificere software. *Fordele*:
  - Er effektive til at fange fejl allerede i specifikations- og design-faserne - sparer penge.

Case Study: Sikringsanlæg



- Et sikringsanlægs opgave er at stille sikre togveje.
- Hvert anlæg (i en produktserie) består typisk af:
  - en generisk software applikation
  - konfigurationsdata (anlægsdata), specificeret i en sporplan + togvejstabel
- Konventionel udvikling og verifikation:
  - *Uformel, manual* udvikling og verifikation af den generiske applikation og konfigurations data.
  - Verifikation af den konfigurerede (specifikke) applikation ved *test*.

Problemer med den Konventionelle Metode

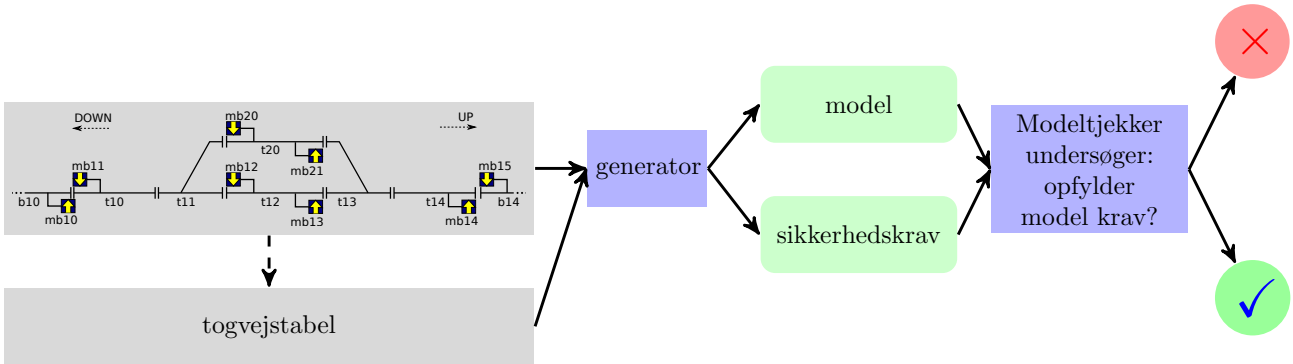


- *Manuel, uformel* specifikation og verifikation er tidskrævende og kan være fejlbehæftet.
- Nogle fejl fanges først ved testning af den konfigurerede (specifikke) applikation, hvilket er dyrt.

$\Rightarrow$ Vi foreslår en metode til *automatiseret, formel* verifikation, der mere effektivt kan fange fejl før implementering og test.

Metode til Formel Verifikation af Sikringsanlæg

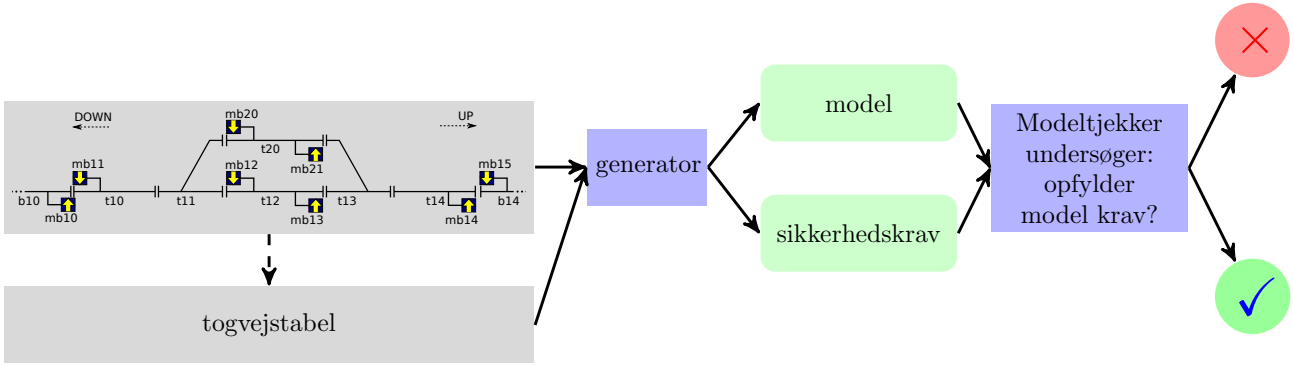
- Et prototype værktøj automatiserer metoden:



1. Input: en sporplan og evt en togvejstabel
2. Værktøjet genererer automatisk en togvejstabel, hvis ej givet som input.
3. Værktøjet checker, at sporplan og togvejstabel er ok.
4. Værktøjet genererer automatisk
   - en formel model M af sikringsanlæggets opførsel og
   - en formalisering af sikkerhedskravene (f.eks. ingen togsammenstød).

5. En modeltjekker undersøger automatisk, om modellen opfylder sikkerhedskravene.
6. Modellen kan desuden bruges til generering af test cases og som test oracle i den senere integrationstest af software implementationen.

Brug af Metoden



- Metoden kan bruges til at finde fejl i sporplaner, togvejstabeller og kontrolalgoritme, allerede i designfasen.
- Metoden har med succes været anvendt til for “early deployment line” Roskilde - Næstved.