RailCons CNL at Chalmers

Bjørnar Luteberget

2016-11-02

Formalizing "Teknisk regelverk"

The Norwegian railway authority has a comprehensive set of technical regulations ("Teknisk regelverk") for design/planning ("prosjektering"), construction, and maintenance of railway infrastructure. The text is also subdivided into 12 disciplines, such as electric, track works, tunnels, and signalling.

Goal

The RailCons project would like to formalize relevant parts of the technical regulations for use in the on-the-fly type of verification which can be used within railway construction design software (specifically the RailCOMPLETE software). This type of verification will probably be limited to static infrastructure analysis, leaving the more heavy-weight analysis of e.g. the implementation of control systems to specialized analysis software such as Prover AB (Sweden) or Systerel (France). However, it could still be beneficial for the method for formalizing the technical regulations to include more dynamic and logically more complex kinds of information, as this could be used to analyse the regulations in themselves, or as input to other types of analysis software.

The suggested use cases are listed here by priority:

1. On-the-fly verification inside the design tool for **static infrastructure**, probably based on the Datalog logic.
2. Control system **implementation verification**, typically more computationally expensive, and based on other formalisms, such as timed automata, first order logic, etc.
3. Verification of human **activities and processes**, such as regulations for maintenance scheduling, or regulations for design *considerations*. (For example, a non-standard design choice for infrastructure could be acceptable only when reasoning has been given for abandoning the standard choice.)
4. Tranforming the regulations into a simpler, unambiguous text for human readers.

Regulations overview

The technical regulations (*"Teknisk regelverk"*) can be found at https://trv.jbv.no/ and consists of the following books:

- **Common regulations**: 501 Common regulations
- **Common electrical**: 510 Design and construction

- **Signs**: 515 Placement of signs along the track
- **Superstructure (tracks)**: 530 Design, 531 Construction, 532 Maintenance
- **Substructure**: 520 Design and construction, 522 Maintenance
- **Tunnels**: 521 Design and construction, 523 Maintenance
- **Bridges**: 525 Design and construction, 527 Maintenance
- **Overhead line**: 540 Design, 541 Construction, 542 Maintenance
- **Low voltage and 22 kV**: 543 Design, 544 Construction, 545 Maintenance
- **Power supply**: 546 Design, 547 Construction, 548 Maintenance
- **Signalling**: 550 Design, 551 Construction, 552 Maintenance, 553 Assessment
- **Telecommunications**: 560 Design and construction, 562 Maintenance

Structure of each book:

- Each book repeats the *common regulations* as the first three chapters.
- Following this will typically be a *general* section containing:
  - declaration of the scope of the book,
  - references to relevant standards,
  - definitions of relevant techincal terms,
  - qualitative classifications, such as quality classes, risk classes, etc.
- The main part of a book consists typically of 5 to 10 chapters, each detailing a specific technical topic within the discipline. The text consists of:
  - Scope declarations
  - Definitions
  - Non-normative statements
  - Comments
  - Regulations (including tables and figures), with exceptions
  - Examples

Scope and focus

The technical regulations contain a lot of generalities which are not necessarily normative, nor directly useful in a design setting. Based on the prioritized use case list, the following parts of the regulations should be considered first in designing and testing the formalization procedure:

1. Superstructure design (track design / *Overbygning: 530 Prosjektering*), especially regulations and formulas regarding
   - track geometry: curvature, gradients, etc.
   - switches: types, maximum speeds, naming (numbering), etc.
2. Signalling design (*Signal: 550 Prosjektering*), especially
   - signal placement, functions, sighting distance
   - train detector placement, classification
   - switch motors requirements and control system components
   - automatic train protection system (ATC) placement and functions
   - interlocking (control system) routes, conflicts, detection sections, safety classes, flank protection, overlaps, etc.

Translation

The technique of controlled natural language will be investigated to allow the input of regulations, especially those translatable into the static infrastructure verification being developed in the RailCons project.

Non-textual information

It could be beneficial to keep tables and figures from the regulations when transitioning to the CNL, so that the CNL interfaces can use these kinds of rich text.

Specifically, referring to figures and referring to the contents of tables based on column and row headers, could be useful.

Examples and relevance

The following table lists some example excerpts from the regulations along with a translation into English, and a comment about use cases and relevance.

Use cases	Original text	English translation	Comments
Overbygning: 530 Prosjektering, Kap. 8 Helsveist spor, 2.1.			
#4	De store krefter som kan forekomme i et helsveist spor stiller strenge krav til sporets konstruksjon.	The large forces that may occur in a welded track makes stringent demands on the track construction.	This sentence is not normative, and is unlikely to have any use in automated verification.
Overbygning: 530 Prosjektering, Kap. 8 Helsveist spor, 2.1.3 a)			
#4	Ballasten skal på linjen og i hovedspor på statsjoner være fullverdig grovpukk (av størrelse 31.5 – 63 mm)	The ballast on the line and in the main track at stations must be purely coarse crushed stone (size from 31.5 to 63 mm)	This is a specification which is absolute, and rules out the need for specifying this as a part of the design, because it is not part of a specific station. It can still be valuable to support this sentence in a CNL, and in a formal representation.
Overbygning: 530 Prosjektering, Kap. 8 Helsveist spor, 2.1.2 a)			
#1	Minste kurveradius for helsveist med betongsviller skal være 250 m.	The lowest allowable radius of curvature for whole welded track on concrete sleepers is 250 m.	This is a typical example of static infrastructure verification, expressible in Datalog as: error(Segment) :- trackSegment(Segment), trackSegmentRadius(Segment, Radius), Radius < 250.

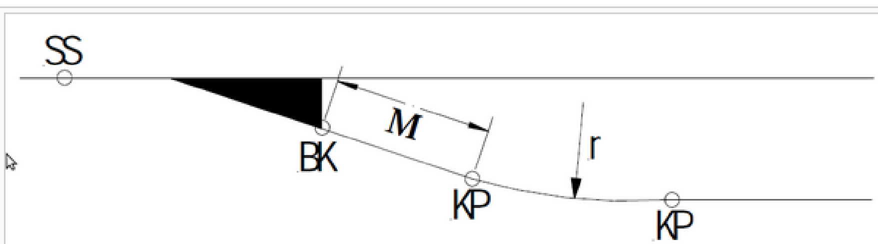
Use cases	Original text	English translation	Comments
Signal: 550 Prosjektering, Kap. 6 Lyssignal, 2.1.2 j)			
#1	Et innkjørhovedsignal skal plasseres $\geq$ 200 meter foran innkjørtogveiens første sentralstilte, motrettede sporveksel, se Figur 5.	A home main signal shall be placed at least 200 m in front of the first controlled, facing switch in the entry train path (see Figure 5).	This is the example that we have been using most frequently for the RailCons verification tool. Datalog: `error(Sig,Sw) :- firstFacing(Bdry, Sw, Dir), homeSignalBetween(Sig, Bdry, Sw), distance(Sig, Sw, Dir, L), L < 200.`
Signal: 550 Signal, Kap. 5 Forriglingsutrustning, 2.8.1 Dekningsgivende objekt			
#1, #2	Følgende objekt kan være dekningsgivende: Hovedsignal, Dvergsignal, Sporveksel, Sporsperre, Avsporingstunge, Signal E35 Stoppskilt. Et hovedsignal skal vise signal "Stopp" for å være dekningsgivende.	The following objects can provide flank protection: main signal, shunting signal, switch, derailer, derailing tongue, signal E35 stop sign. A main signal must display "stop" to provide flank protection.	This regulation is relevant both for **specifying** the control system, and for verifying the **implementation**. The specification chooses which objects to use for flank protection (**static**) and what state they can be used in, while the implementation must correctly enforce the conditions saying which message the signal displays (**dynamic**).
Signal: 550 Prosjektering, Kap. 6 Lyssignal, 2.1.2 i)			
#1, #3	Et hovedsignal bør ikke plasseres i tunneler, på bruer, eller andre steder hvor en eventuell togstans og dermed muligheten for avstigning, vil medføre fare.	A main signal should not be placed in tunnels, on bridges, or other places where halting trains and thus the possibility of disembarking, can impose dangers.	Here we have an example of a "*should*" modality, where the static infrastructure verification could issue a warning, but not an error. Also, it could be required to document the alternatives that were considered when deciding on the design.
Signal: 550 Prosjektering, Kap. 5 Forriglingsutrustning, 4.1.1.1 i)			
#2	For at en togvei skal kunne fastlegges, skal et objekt som gir dekning til togveien være dekningsgivende.	For a train route to be deactivated, any object giving flank protection must be in a protecting state.	This regulation concerns only the state of the control system, and as such relates to the implementation of the control system and not the static infrastructure specification.

Use cases	Original text	English translation	Comments
Overbygning: 530 Prosjektering, Kap. 5 Sporets trasé, 3.1 Dimensjonerende parametre			
#1	See table below.	(a) minimum radius, (b) maximal superelevation, (c) limit on superelevation cause by derailment risk at low speeds, (d) limit for superelevation rate of change, (e) limit for superelevation deficit.	Limiting values are organized in a table for use in formulas in other sections.

Tabell 2: Dimensjonerende parametre for nye baner og linjeomlegginger

	Symbol	Definisjon	Normale krav	Minste krav
a)	$R_{\min}$	minste radius	250 m	190 m
b)	h_{maks}	maksimal verdi for overhøyden 1)	150 mm	
c)	h_{avsp}	grense for overhøyde pga. avsporingsfaren ved lave hastigheter	$\frac{R-100}{2}$ mm	
d)	$\left(\frac{\Delta h}{L}\right)_{maks}$	grenseverdi for rampestigning	1:400	
e)	I_{maks}	grenseverdi for manglende overhøyde 2)	R ≤ 600: 100 mm R > 600: 130 mm	

Use cases	Original text	English translation	Comments
Overbygning: 530 Prosjektering, Kap. 5 Sporets trasé, 3.7 Sporveksler og sporforbindelser			
#1	Avstanden mellom sporveksel og overgangskurve, sirkelkurve, bru eller annen motstående sporveksel skal ikke være mindre enn avstanden M gitt i *Kurver uten overgangskurver*, krav b). M skal imidlertid ikke være kortere enn 6 m.	The distance between the switch point and the transition curve, circle curve, bridge or other opposite switch point should not be less than the distance M given in section *"curves without transition curves"*, requirements b). M shall not be shorter than 6 m.	The parameter M is explained by the figure below. Reference is given to another section of the regulations.



Figur 4: Krav til rettlinje M ved linjedelende sporveksel

Use cases	Original text	English translation	Comments
Overbygning: 530 Prosjektering, Kap. 5 Sporets trasé, 5 Største hastighet – sporets geometri			
#1	Hastigheten i en kurve skal ikke være større enn: $V = 0,291 \cdot \sqrt{R\,(h + I_{\text{maks}})}$ (5) Hvis ligning 5 i tilfeller med falsk overhøyde gir lavere verdi enn 20 km/h gjelder $V = 20$ km/h.	The speed in a curve shall not exceed: $V = 0,291 \cdot \sqrt{R\,(h + I_{\text{maks}})}$ (5) If Eq. 5 gives a lower value than 20 km/h in situations with false superelevation, then $V = 20$ km/h shall be used.	Use of equations with designed and given parameters.
Signal: 552 Vedlikehold, Kap. 6 Lyssignal, 3 Lyssignaler			
#3, #4	Dersom lyssignal er vridd eller på annen måte kommet ut av stilling skal dette utbedres snarest.	If a signal is twisted or in other ways are out of position, this shall be fixed as soon as possible.	Typical maintenance regulation. Here, it might be sufficient to identify this as a *checklist item*, for maintenance scheduling and reporting purposes.