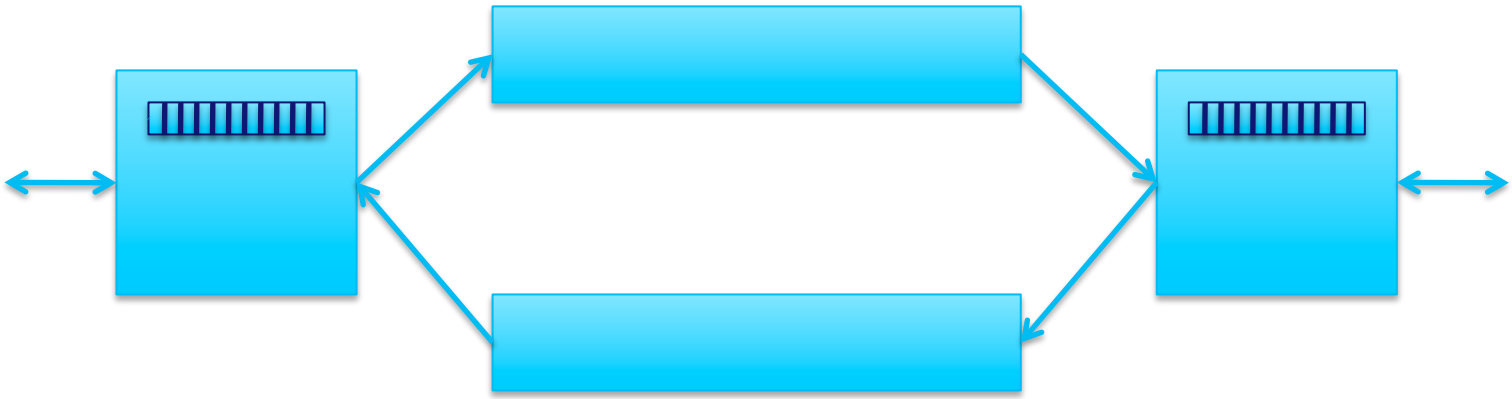
ERTMS en softwareveiligheid.

Jan Friso Groote

Technische Universiteit
Eindhoven
University of Technology

Where innovation starts

Software is raar spul: een anecdote....



Sliding window protocol. Tanenbaum's Computer Networks

>>10^{2500} states

Software is raar spul.

- Het aantal states is >> astronomisch
  (astronomische getallen → informaticagetallen).
- Veel voorkomende problemen worden wel gevonden door te testen (99% goed is eenvoudig bereikbaar).
- Weinig voorkomende problemen kunnen zich pas na jaren manifesteren.
- Goed functionerende systemen zijn niet gegarandeerd bestand tegen opzettelijk misbruik.

Informele beschrijvingen van software zijn foutgevoelig

4.4.9 FULL SUPERVISION

4.4.9.1 Description

4.4.9.1.1 The ERTMS/ETCS on-board equipment shall be in the Full Supervision mode when all train and track data, which is required for a complete supervision of the train, is available on board.

4.4.9.1.2 Full supervision cannot be selected by the driver, but shall be entered automatically when all necessary conditions are fulfilled.

4.4.9.1.3 To be in Full Supervision mode, SSP and gradient are not required for the whole length of the train, but shall be at least available from the FRONT END of the train.

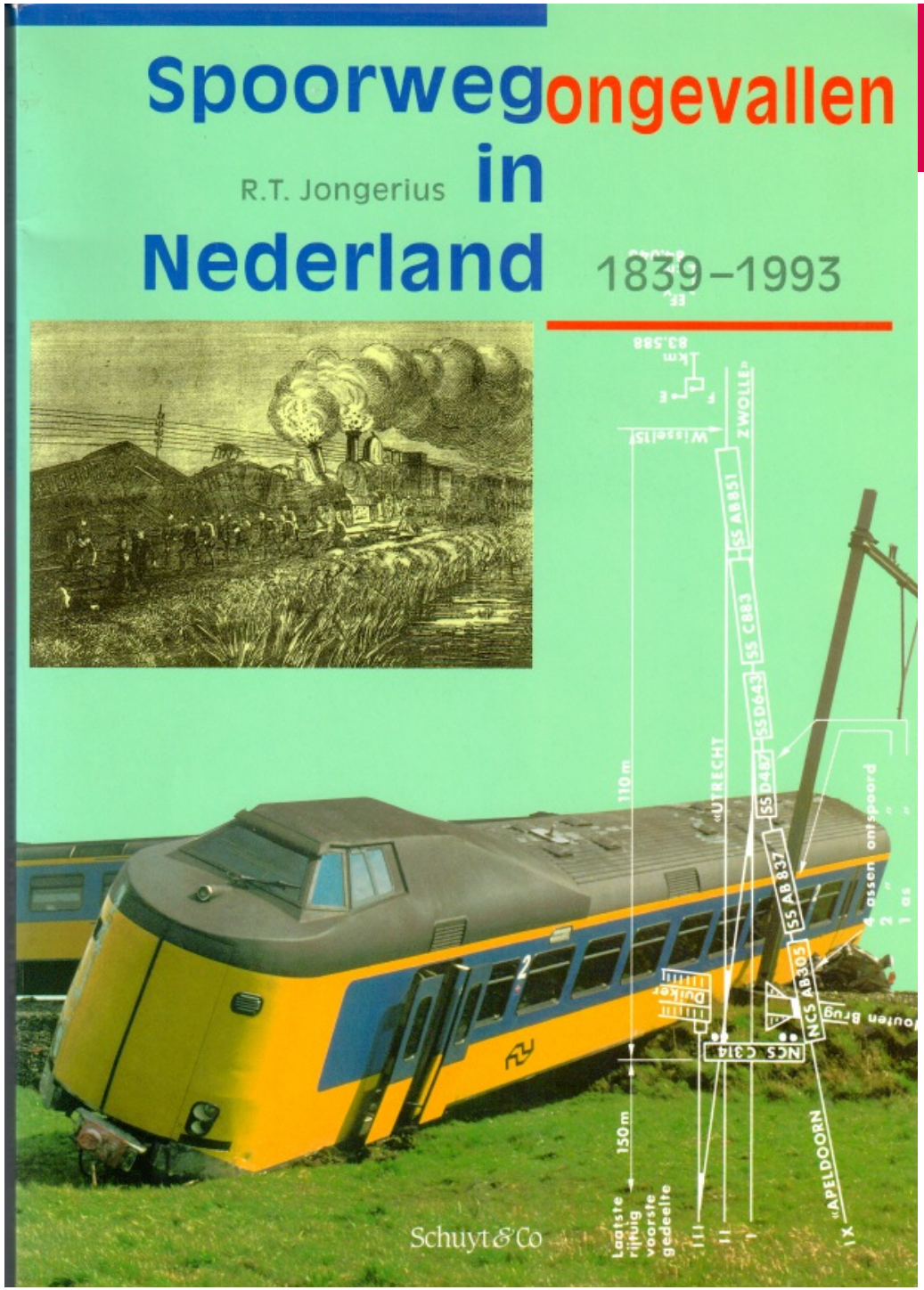
4.4.9.1.4 Once in Full Supervision mode, if SSP and gradient are not known for the whole length of the train, an indication “ENTRY IN FULL SUPERVISION” shall be clearly displayed to the driver until SSP and gradient are known for the whole length of the train.

4.4.9.1.4.1 Note: this indication may also be displayed in case the train length has been increased, see 3.18.3.8.

4.4.9.1.5 The ERTMS/ETCS on-board equipment shall supervise train movements against a dynamic speed profile.

4.4.9.1.6 The ERTMS/ETCS on-board equipment shall display the train speed, the permitted speed, the target distance and the target speed to the driver (this list is not exhaustive – refer to chapter 4.7 “DMI depending on modes”).

4.4.9.1.7 Note: for the list of main functions related to this mode, refer to chapter 4.5 “Modes and on-board functions”.



Alle ongelukken met minimaal
1 passagier als slachtoffer +
Harlingen 1868.

Spoor werd steeds veiliger.

Informele beschrijvingen van software zijn foutgevoelig

4.4.9 FULL SUPERVISION

4.4.9.1 Description

4.4.9.1.1 The ERTMS/ETCS on-board equipment shall be in the Full Supervision mode when all train and track data, which is required for a complete supervision of the train, is available on board.

4.4.9.1.2 Full supervision cannot be selected by the driver, but shall be entered automatically when all necessary conditions are fulfilled.

4.4.9.1.3 To be in Full Supervision mode, SSP and gradient are not required for the whole length of the train, but shall be at least available from the FRONT END of the train.

4.4.9.1.4 Once in Full Supervision mode, if SSP and gradient are not known for the whole length of the train, an indication “ENTRY IN FULL SUPERVISION” shall be clearly displayed to the driver until SSP and gradient are known for the whole length of the train.

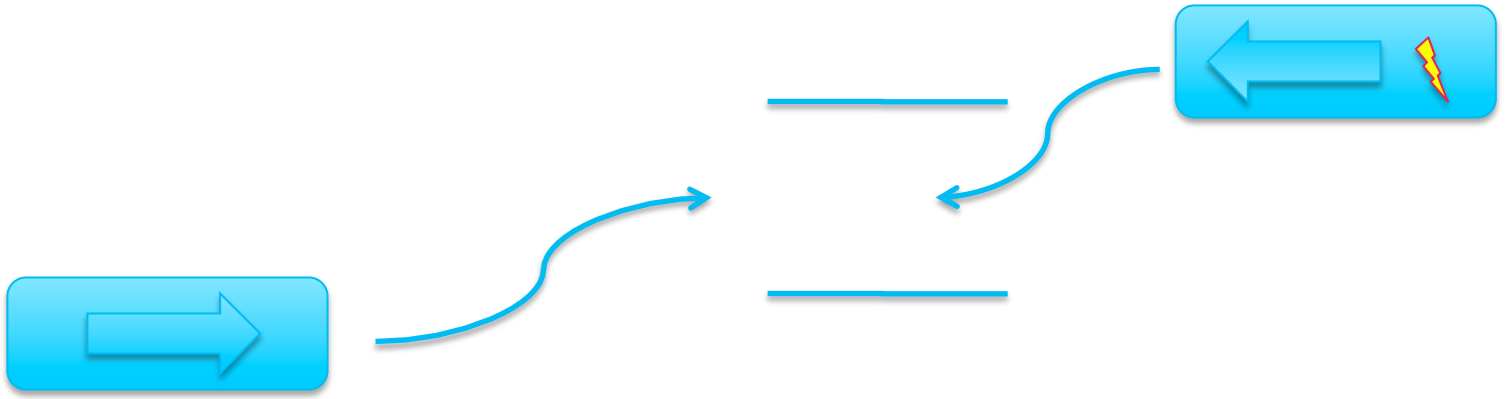
4.4.9.1.4.1 Note: this indication may also be displayed in case the train length has been increased, see 3.18.3.8.

4.4.9.1.5 The ERTMS/ETCS on-board equipment shall supervise train movements against a dynamic speed profile.

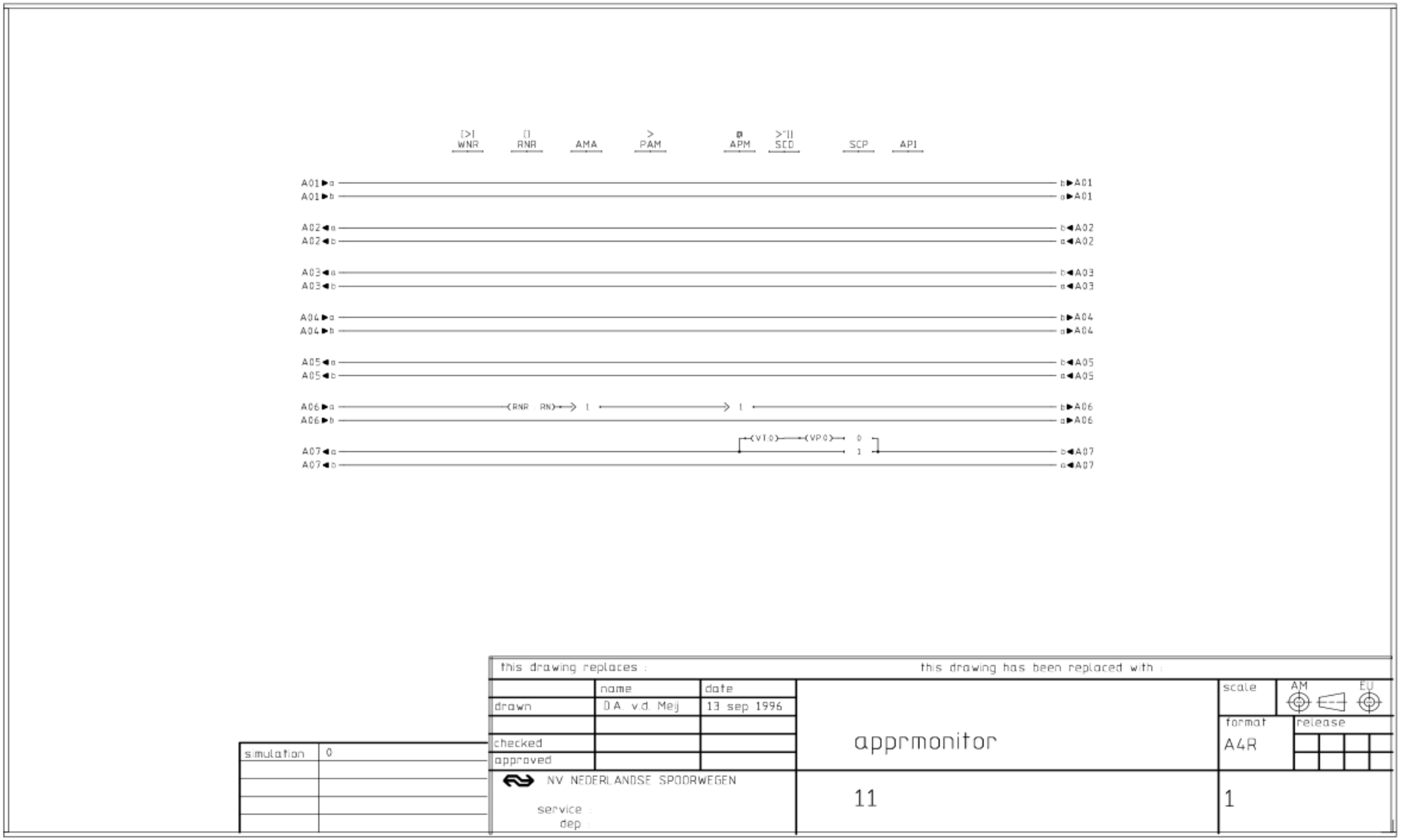
4.4.9.1.6 The ERTMS/ETCS on-board equipment shall display the train speed, the permitted speed, the target distance and the target speed to the driver (this list is not exhaustive – refer to chapter 4.7 “DMI depending on modes”).

4.4.9.1.7 Note: for the list of main functions related to this mode, refer to chapter 4.5 “Modes and on-board functions”.

Autonome bussen, Zuid Holland

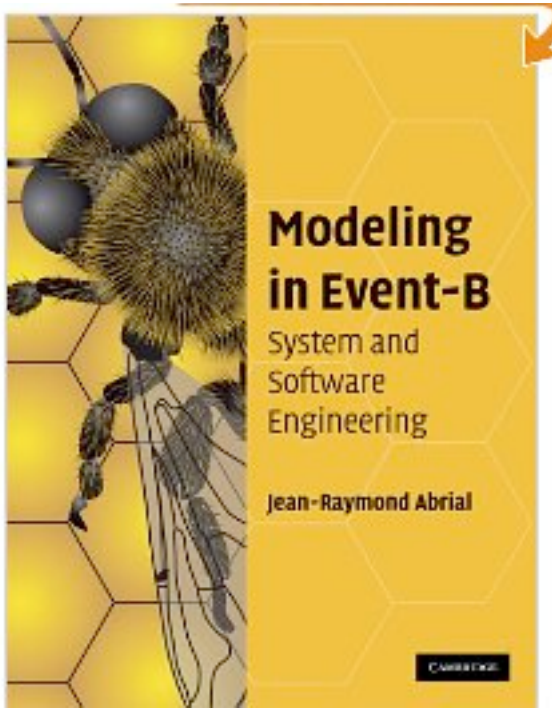


Euris; Peter Middelraad



/tmp_mnt/home/euris/guide_top/unispec/lscdestop/apprmonitor/apprmonitor.sbk(01;15) Mon Dec 1 10:49:02 1997

Onbemande Metro in Parijs.



Metro lijn 14 in Parijs.

Geheel ontwikkeld in B. Eerst dmv.
invarianten correct bewezen.
Tot nu toe geen software problemen ontdekt.

Vergelijkend warenonderzoek.

Formele specificatie versus klassiek design

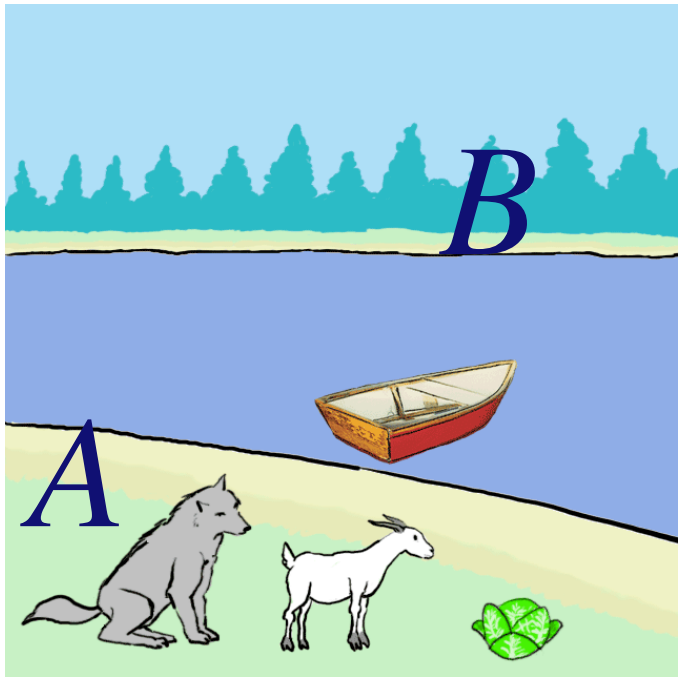
Tot 10x minder fouten tijdens ontwikkeling.

Tot 3x snellere ontwikkeltijd; nooit langzamer.

Hoe bestudeer je communicatie protocollen

Flaccus Albinus Alcuinus
Propositiones ad acuendos iuuenes, 7de eeuw.

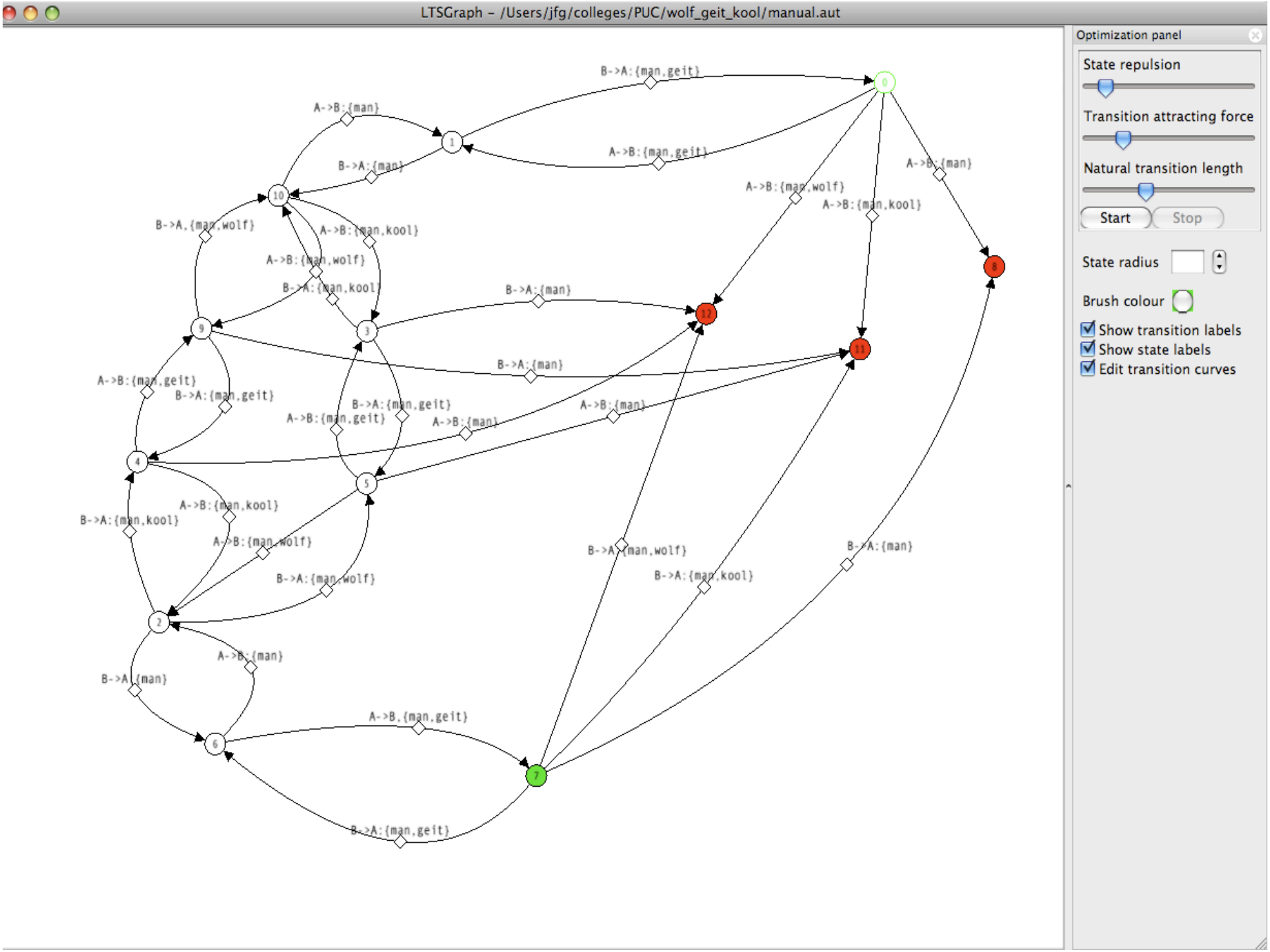
$$A \rightarrow B : \{Man, Wolf\}$$
$$B \rightarrow A : \{Man\}$$
$$A \rightarrow B : \{Man\ Geit\}$$
$$B \rightarrow A : \{Man\}$$
$$A \rightarrow B : \{Man, Kool\}$$



Maak een beschrijving van alle mogelijke ‘berichtenuitwisselingen’.

mcrl2 toolset
www.mcrl2.org

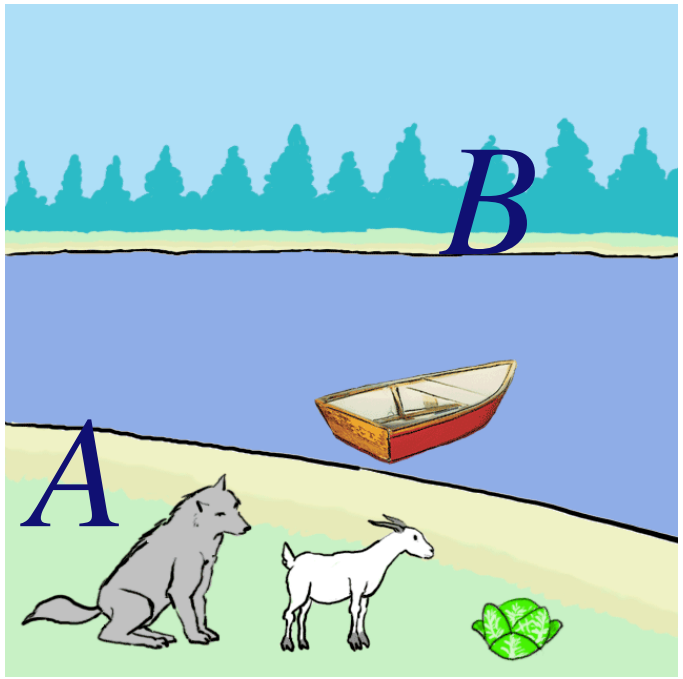
mCRL2
analysing system behaviour


LTSGraph – /Users/jfg/colleges/PUC/wolf_geit_kool/manual.aut
Optimization panel
State repulsion
Transition attracting force
Natural transition length
Start
Stop
State radius
Brush colour
Show transition labels
Show state labels
Edit transition curves
B->A:{man,geit}
A->B:{man}
A->B:{man,geit}
B->A:{man}
A->B:{man}
A->B:{man,wolf}
A->B:{man,kool}
B->A:{man,wolf}
A->B:{man,kool}
B->A:{man,wolf}
B->A:{man,kool}
B->A:{man}
B->A:{man}
A->B:{man,geit}
B->A:{man,geit}
A->B:{man,geit}
B->A:{man,geit}
A->B:{man}
A->B:{man}
A->B:{man,kool}
B->A:{man,kool}
A->B:{man,wolf}
B->A:{man,wolf}
B->A:{man,wolf}
B->A:{man,kool}
B->A:{man}
A->B:{man}
B->A:{man}
A->B:{man,geit}
B->A:{man,geit}

Modale logica

Flaccus Albinus Alcuinus
Propositiones ad acuendos iuuenes, 7de eeuw.

$$A \rightarrow B : \{Man, Wolf\}$$
$$B \rightarrow A : \{Man\}$$
$$A \rightarrow B : \{Man\ Geit\}$$
$$B \rightarrow A : \{Man\}$$
$$A \rightarrow B : \{Man, Kool\}$$

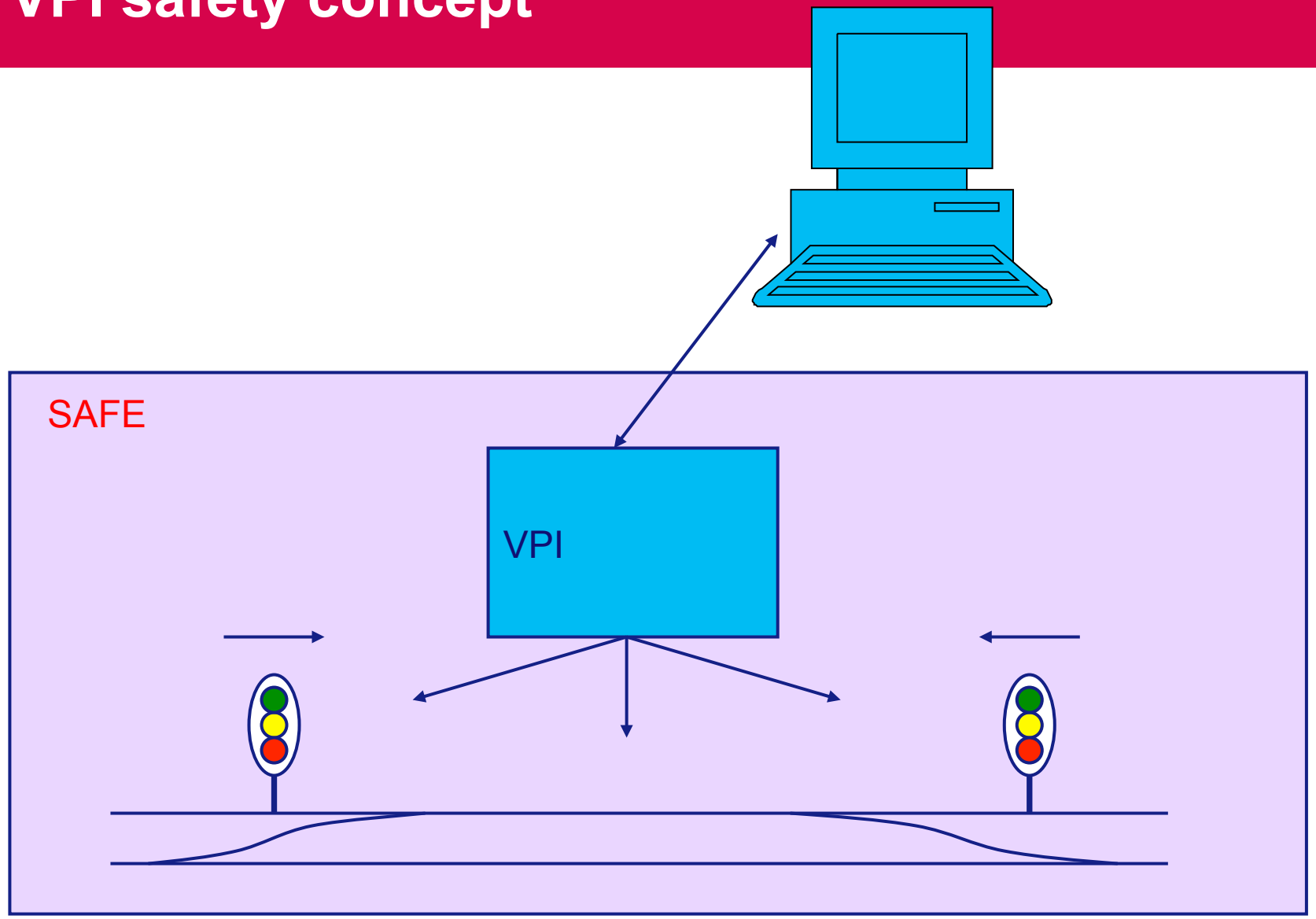


Check de volgende modale formule:

overkant: iedereen is aan de overkant
opgegeten: de geit of kool wordt opgegeten

$$\mu X.(\langle overkant \rangle true \vee \langle true \rangle X) \wedge [opgegeten] false$$

VPI safety concept



2000 lines for Heerhugowaard

10^{1000} states

```
APPLICATION = LAMPSTURING SEINEN
BOOL 1254-GR-ACO    = (1254-GR)
BOOL 1254-GRFL-ACO  = (1254-GRFL)
BOOL 1254-GL-ACO = ((1254-GL + 1254-GL4 + 1254-GL6) *
                                  .N.1254-GR-ACO * .N.1254-GRFL-ACO)
BOOL 1254-4-ACO     = (1254-GL4 * 1254-GL-ACO)
BOOL 1254-6-ACO     = (1254-GL6 * 1254-GL-ACO)
BOOL 1254-4/6-ACO   = ((1254-GL4 + 1254-GL6) * 1254-GL-ACO)
BOOL 1254-GLFL-ACO  = (1254-GLFL)
BOOL 1254-R-ACO= (.N.1254-GLFL-ACO * .N.1254-GL-ACO *
                                  .N.1254-GRFL-ACO * .N.1254-GR-ACO)
```

Requirements on a VPI

Two signals directed to each other should not both show green or yellow at the same time.

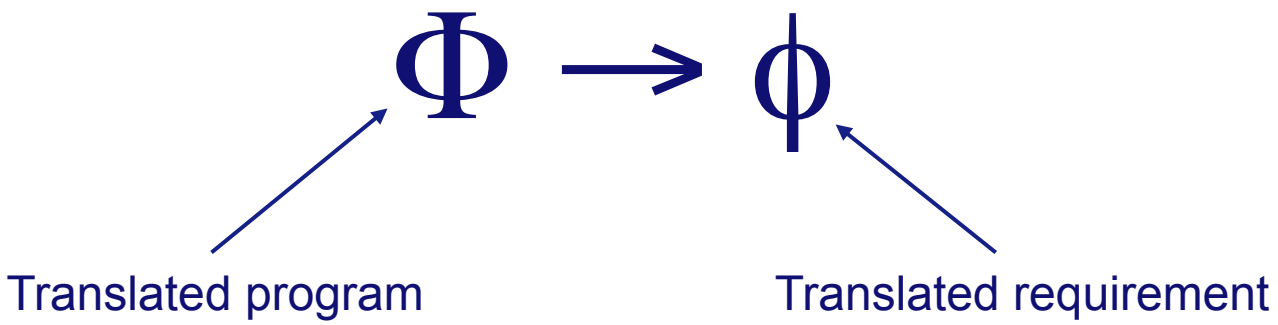
A signal to an occupied track shall not show green.

A switch cannot move if a train is allowed to pass.

A green signal is never followed by a red signal.

W.J. Fokkink. Safety criteria for the vital processor interlocking at Hoorn-Kersenboogerd. Comprail 96

How to verify the requirements: Translate to propositional logic.



Verification of such properties requires a few seconds.
Tools: Prover, Heerhugo, Grasp, Sato, Chaff, Minisat,…

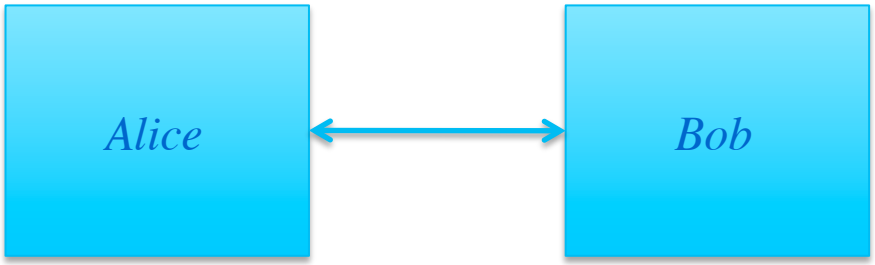
actually used

Algerabrug: Krimpen aan de IJssel.

Op gelijke wijze:
Complete analyse van de source code van de Algerabrug

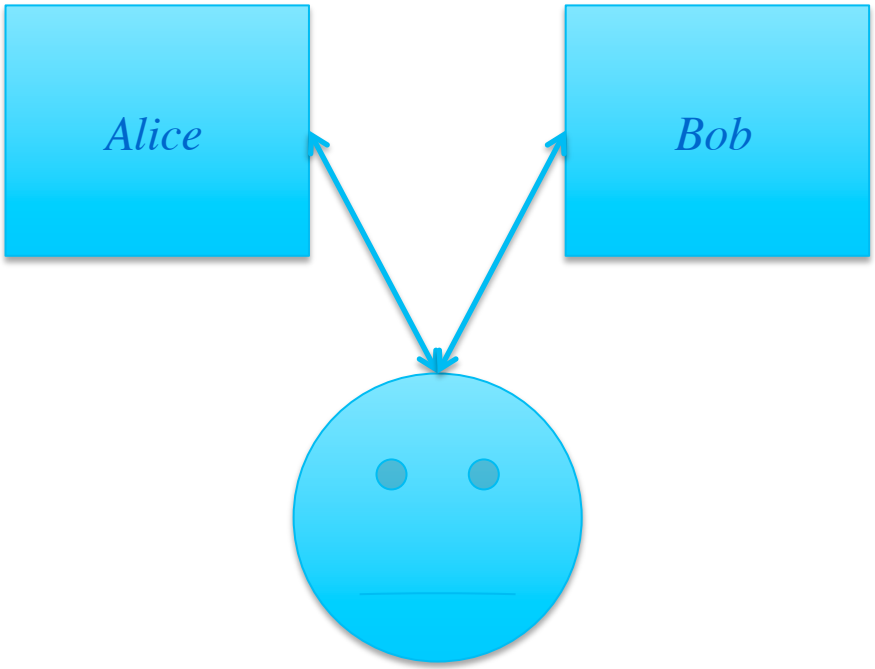
Inmiddels werken we aan de compleet geformaliseerde aansturing van de modelbrug, partieelcorrect bewezen tov. veiligheids- en functionaliteits-eisen.

Veiligheid: “Security” is moeilijker dan “Safety”



De meeste “security” problemen zijn terug te voeren op incompetentie.
Diginotar, websites, flauwe passwords....
De volgende categorie misbruikt software bugs.
Maar weinig zijn gebaseerd op fouten in het design van security protocollen.

Veiligheid: “Security” is moeilijker dan “Safety”



Intruder luistert mee en kan gebruiken wat hij heeft gehoord.

Redundancy in messages is dangerous

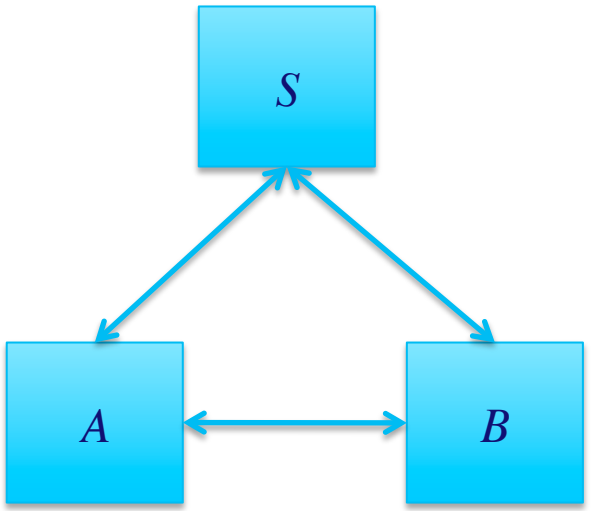
ERTMS: Messages are 64 bits long and encrypted using the triple key method.
Messages that are shorter than 64 bits are padded with zero's.

Enigma: gekraakt door Polen
in 1938, voor de Duitse inval.

Het symmetrische Needham-Schroeder protocol

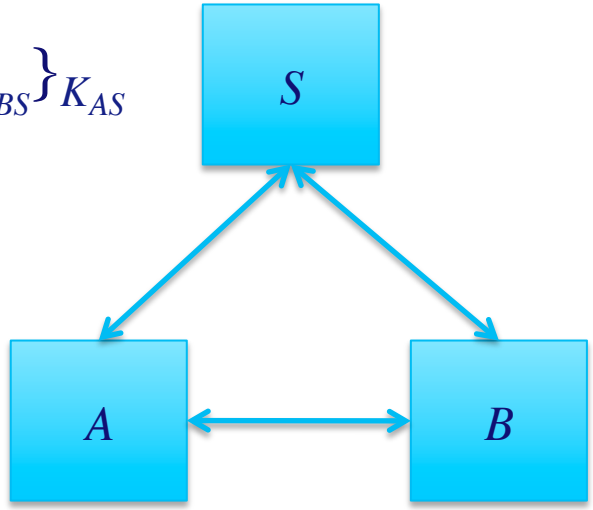
Doel: een server S moet een symmetrische sessiesleutel K_{AB} aan A en B verstrekken

$$A \rightarrow S : A, B, N_A$$
$$S \rightarrow A : \{N_A, K_{AB}, B, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$$
$$A \rightarrow B : \{K_{AB}, A\}_{K_{BS}}$$
$$B \rightarrow A : \{N_B\}_{K_{AB}}$$
$$A \rightarrow B : \{N_B\text{-}1\}_{K_{AB}}$$



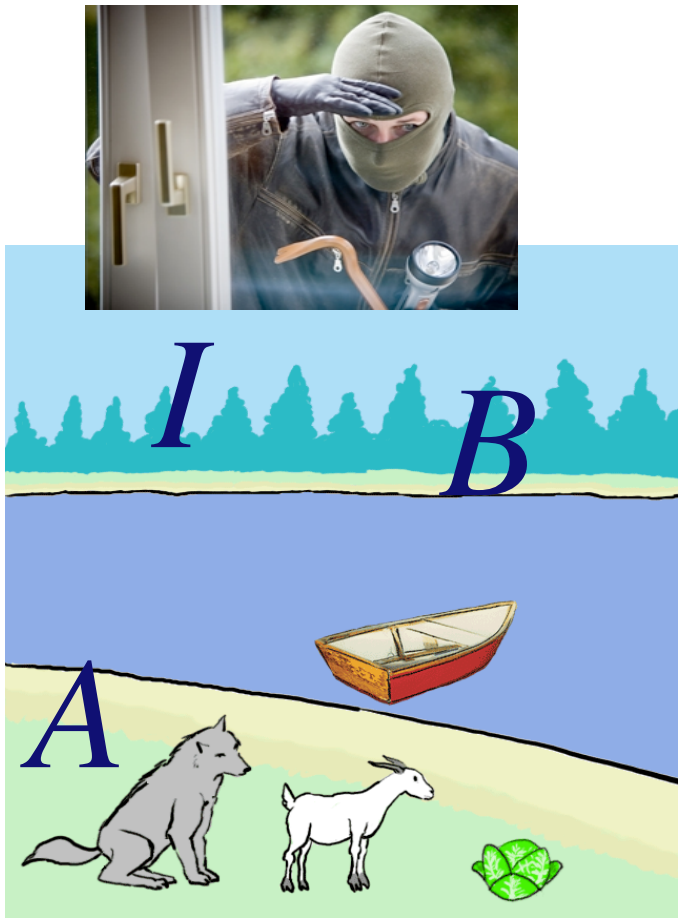
Reparatie van het Needham-Schroeder protocol

$$A \rightarrow B : A$$
$$B \rightarrow A : \{A, N'_B\}_{K_{BS}}$$
$$A \rightarrow S : A, B, N_A, \{A, N'_B\}_{K_{BS}}$$
$$S \rightarrow A : \{N_A, K_{AB}, B, \{K_{AB}, A, N'_B\}_{K_{BS}}\}_{K_{AS}}$$
$$A \rightarrow B : \{K_{AB}, A, N'_B\}_{K_{BS}}$$
$$B \rightarrow A : \{N_B\}_{K_{AB}}$$
$$A \rightarrow B : \{N_B\text{-}1\}_{K_{AB}}$$

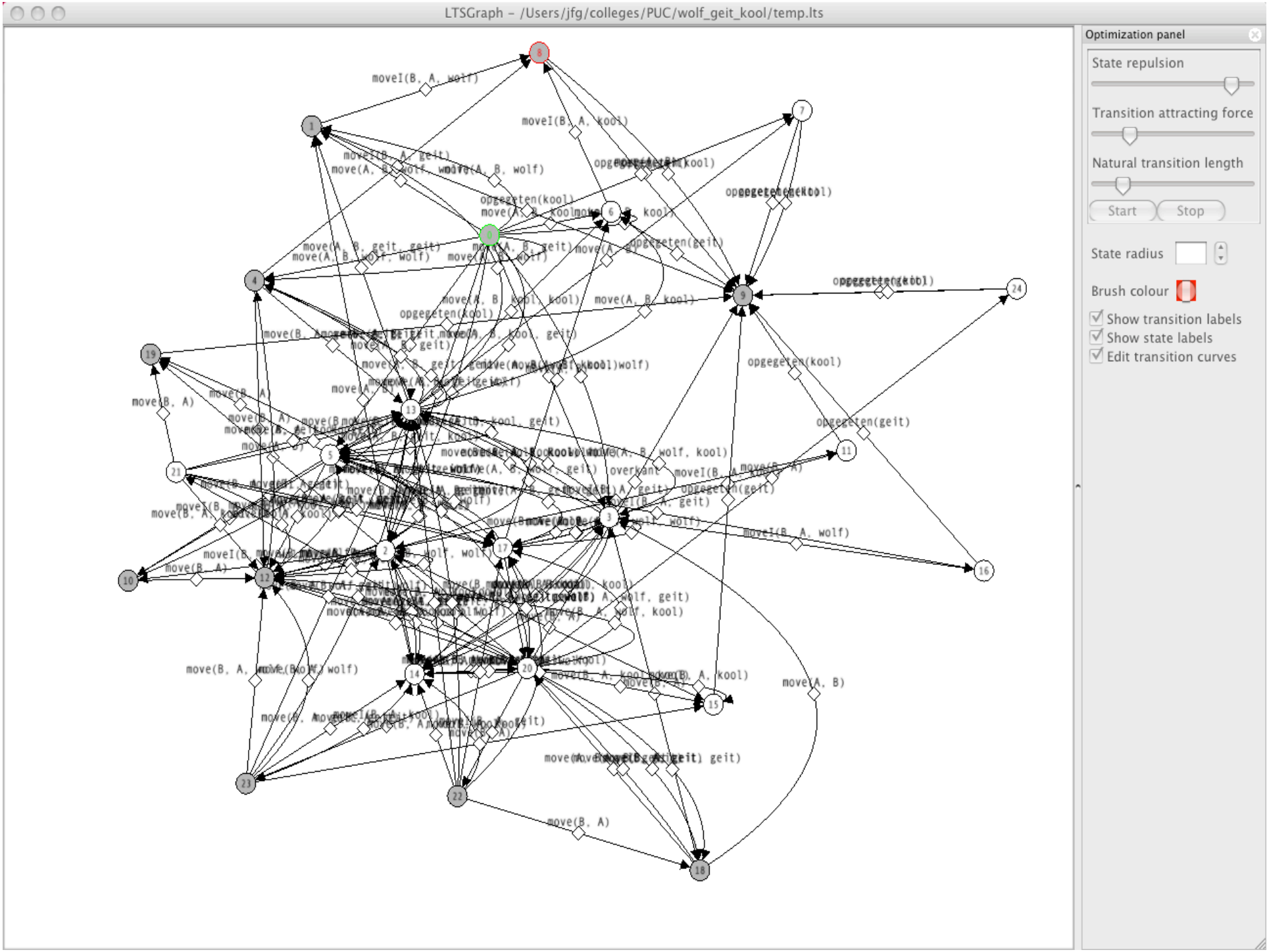


Nu met intruder

Flaccus Albinus Alcuinus
Propositiones ad acuendos iuuenes, 7de eeuw.

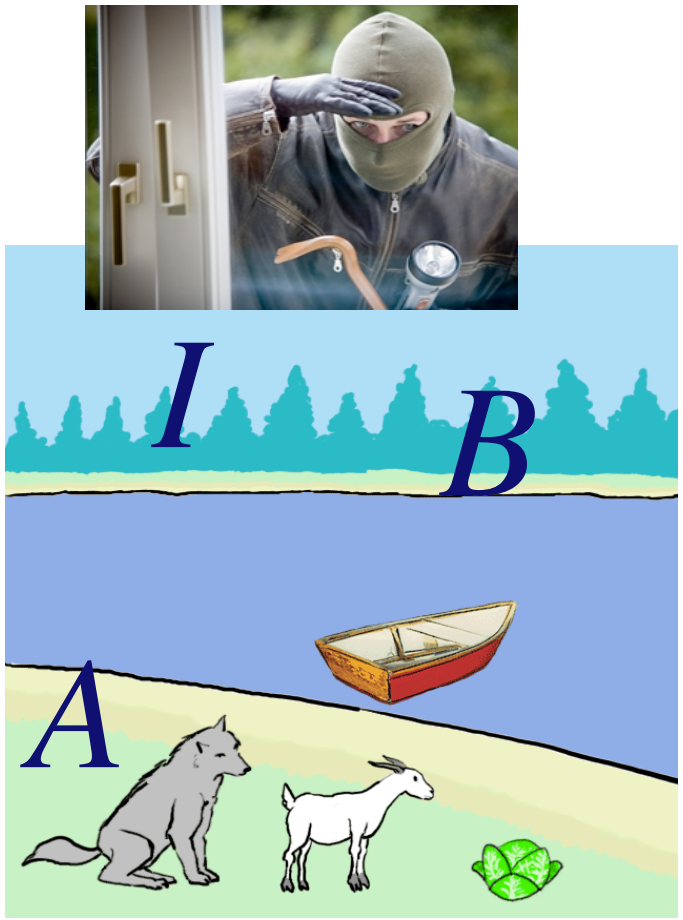


$$A \rightarrow B : \{Man, Wolf, Kool\}$$
$$B \rightarrow A : \{Man\}$$
$$B \rightarrow I : \{Wolf\}$$
$$I \rightarrow A : \{Wolf\}$$
$$A \rightarrow B : \{Man\ Geit\}$$
$$B \rightarrow A : \{Man\}$$
$$A \rightarrow B : \{Man, Kool\}$$
$$\ldots\ldots\ldots$$


LTSGraph - /Users/jfg/colleges/PUC/wolf_geit_kool/temp.lts
Optimization panel
State repulsion
Transition attracting force
Natural transition length
Start
Stop
State radius
Brush colour
Show transition labels
Show state labels
Edit transition curves
moveI(B, A, wolf)
moveI(B, A, kool)
moveI(B, A, geit)
move(A, B, wolf)
opgegeten(kool)
opgegeten(geit)
move(A, B, kool)
move(A, B, geit)
move(B, A)
move(A, B)
overkant
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

Nu met intruder

Flaccus Albinus Alcuinus
Propositiones ad acuendos iuuenes, 7de eeuw.



$A \rightarrow B : \{Man, Wolf, Kool\}$
$B \rightarrow A : \{Man\}$
$B \rightarrow I : \{Wolf\}$
$I \rightarrow A : \{Wolf\}$
$A \rightarrow B : \{Man\ Geit\}$
$B \rightarrow A : \{Man\}$
$A \rightarrow B : \{Man, Kool\}$
.....

$mu\ X.($<overkant>$true \vee$
$(\langle A \rightarrow B \rangle X \wedge$
$[B \rightarrow I \rightarrow A\ ]X)$
$) \wedge$ [opgegeten]$false$

NIET WAAR

Wat moeten/kunnen we doen?

- Formaliseer de ERTMS protocollen. Maak heel precies welke component welk telegram wanneer stuurt.
- Formaliseer de veiligheid (safety). Wat mag nooit en wat moet er altijd gebeuren. Bewijs (formeel) dat de protocollen aan de veiligheidseisen voldoen.
- Formaliseer security. Bewijs dat intruders geen kans hebben.
- Dit is allemaal niet eenvoudig. En we zoeken naar die fouten die sowieso niet heel vaak voorkomen.