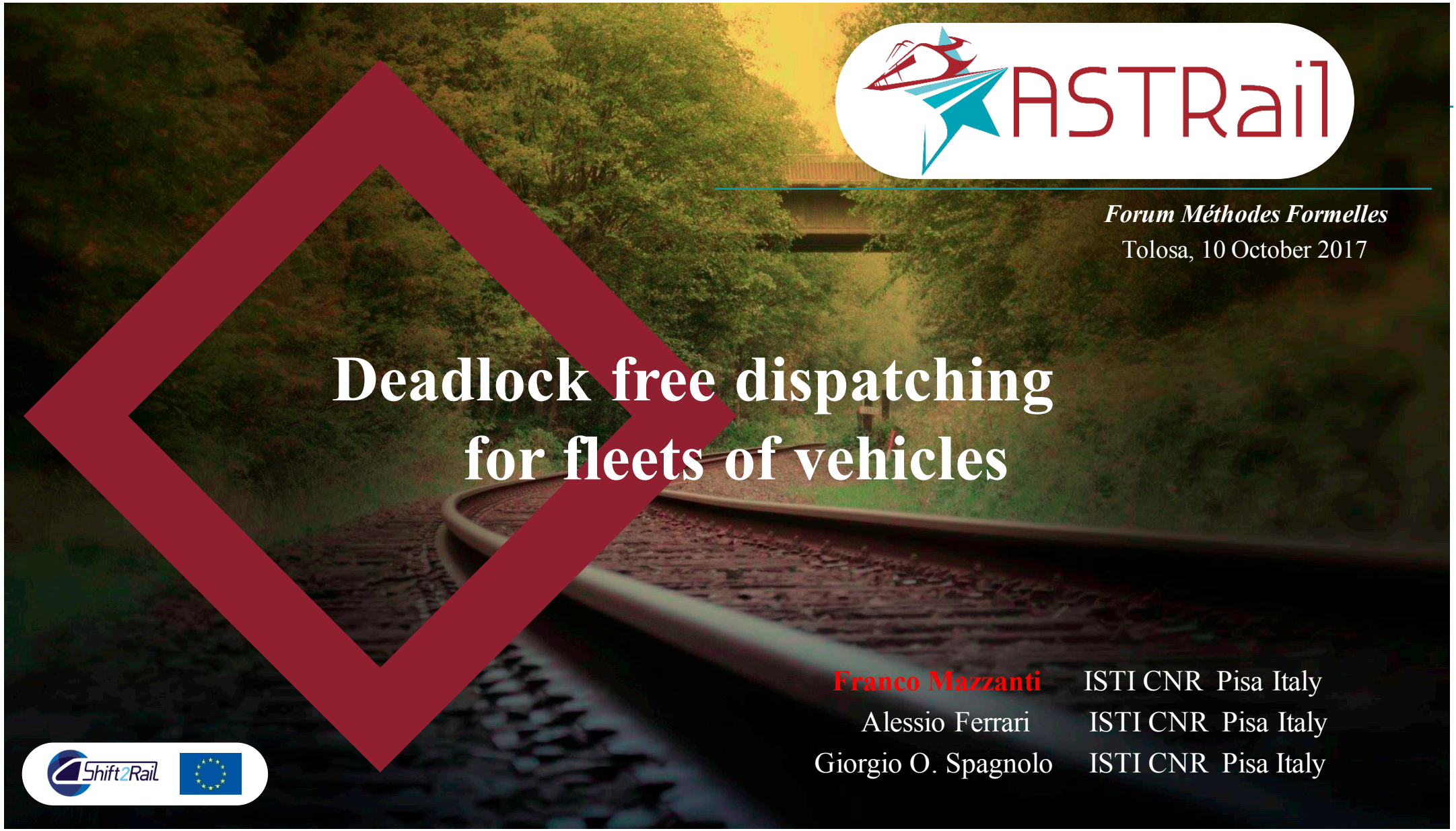


Forum Méthodes Formelles
Tolosa, 10 October 2017

Deadlock free dispatching for fleets of vehicles

Franco Mazzanti ISTI CNR Pisa Italy
Alessio Ferrari ISTI CNR Pisa Italy
Giorgio O. Spagnolo ISTI CNR Pisa Italy

Presentation

CONSIGLIO NAZIONALE DELLE RICERCHE

ISTITUTO DI SCIENZA E TECNOLOGIE DELL'INFORMAZIONE "A. FAEDO"

FORMAL METHODS && TOOLS LABORATORY

Franco Mazzanti

Senior Researcher

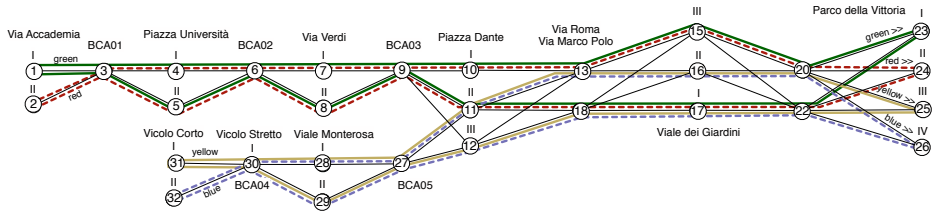
http://fmt.isti.cnr.it

KandISTI 2017 - Open Access

http://fmt.isti.cnr.it/kandisti

TraCE - IT

Train **C**ontrol **E**nhancement via **I**nformation **T**echnology



The original TRACE-IT goal:

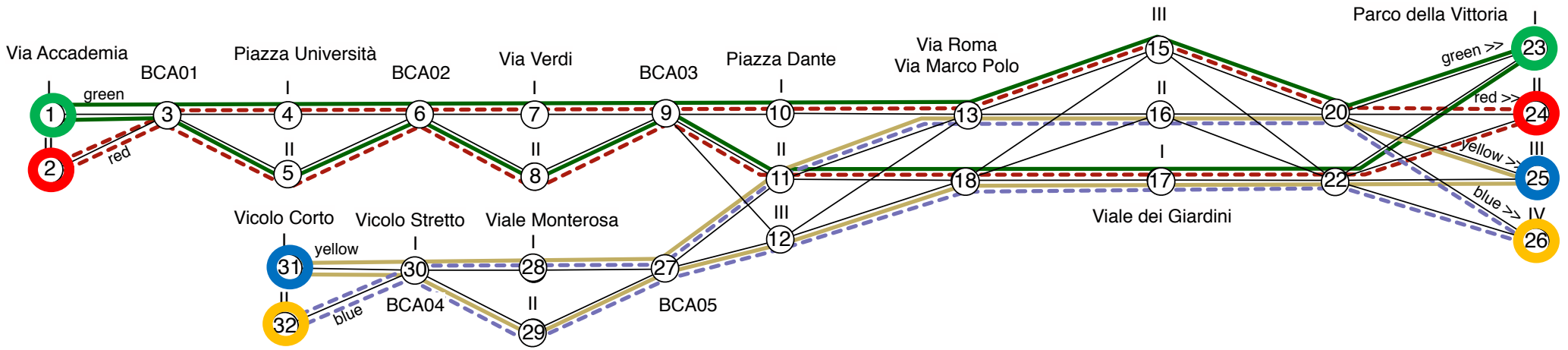
Design an ATS (Automatic Train Supervision) System that:

- Controls the dispatching of a set trains on a railway layout
- Handling a continuously running set of circular train missions
- Preventing the occurrence of (partial) deadlocks.

Safety of the system is guaranteed by the ATP / Interlocking systems

What we have here is essentially a problem of (mission critical) liveness

The original case study



- We have a metro service: 8 trains providing circular services


[1,3,4,6,7,9,10,13,15,20,23,22,17,18,11,9,8,6,5,3,1]



[2,3,4,6,7,9,10,13,15,20,24,22,17,18,11,9,8,6,5,3,2]

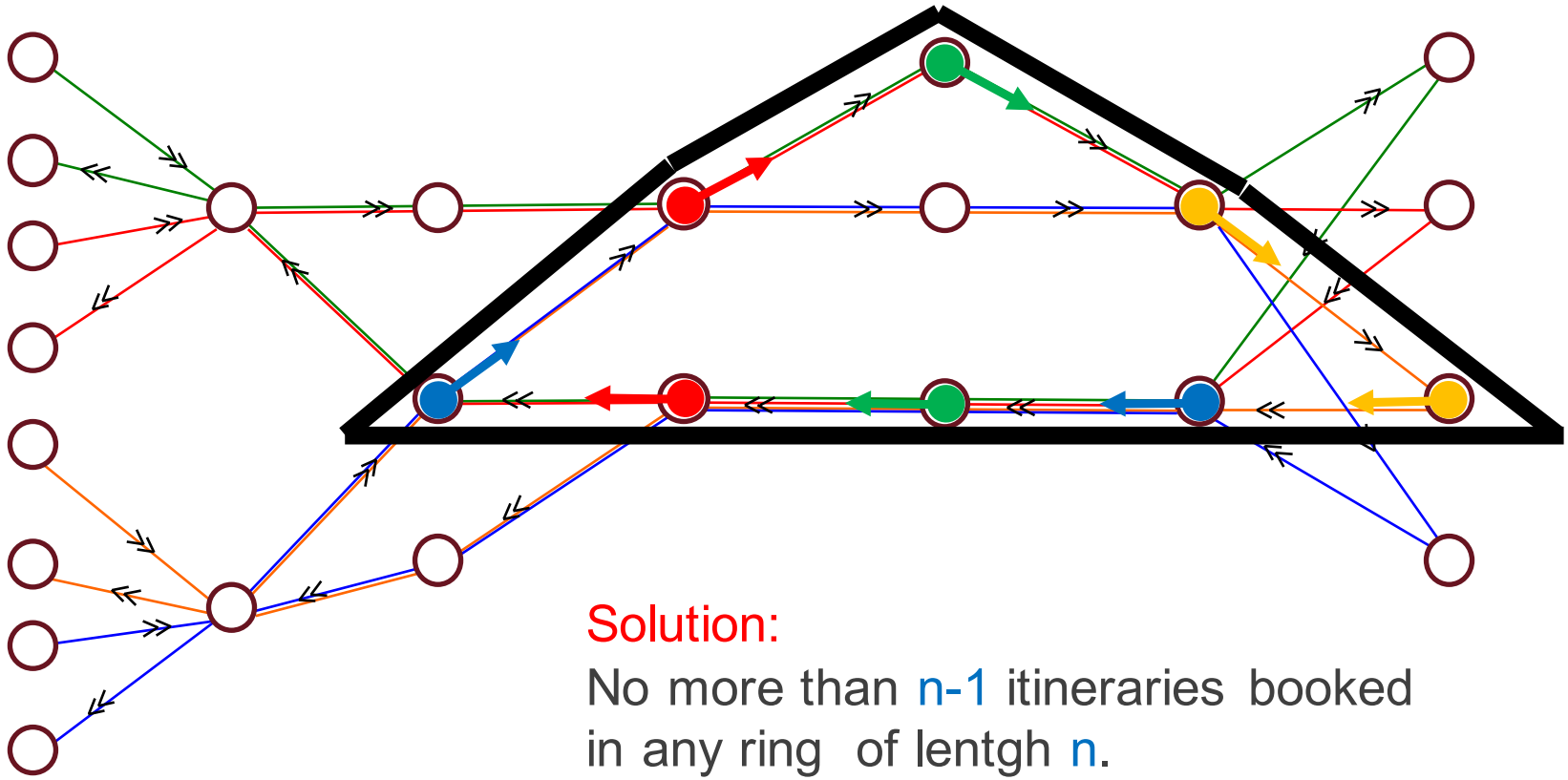


[31,30,28,27,11,13,15,20,25,22,17,18,12,27,29,30,31]



[32,30,28,27,11,13,15,20,26,22,17,18,12,27,29,30,32]

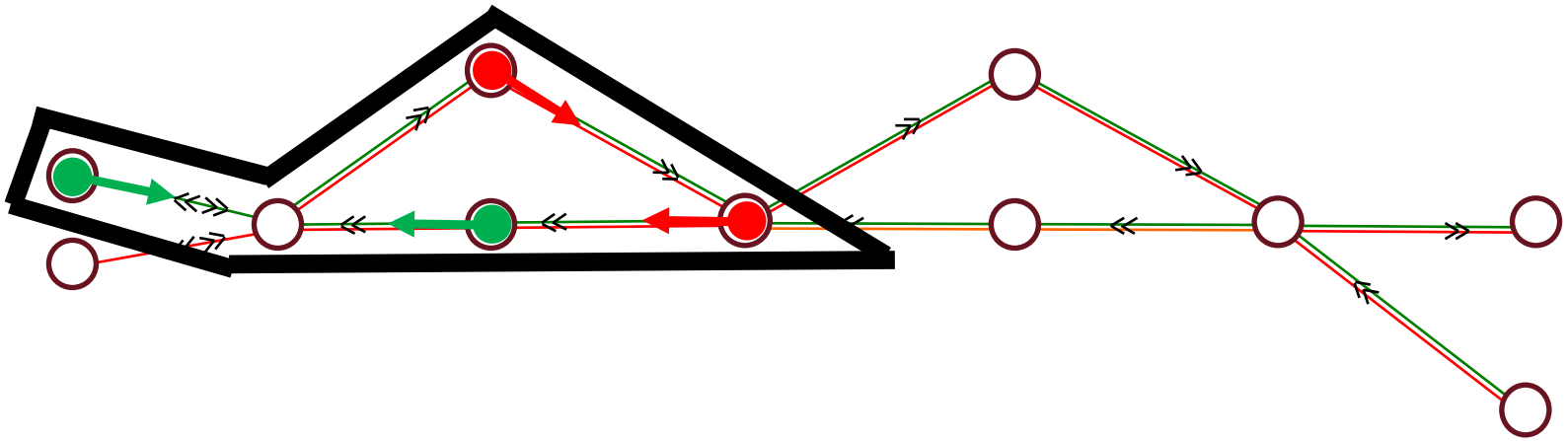

Deadlock on basic sections



Solution:

No more than n-1 itineraries booked in any ring of lentgh n.

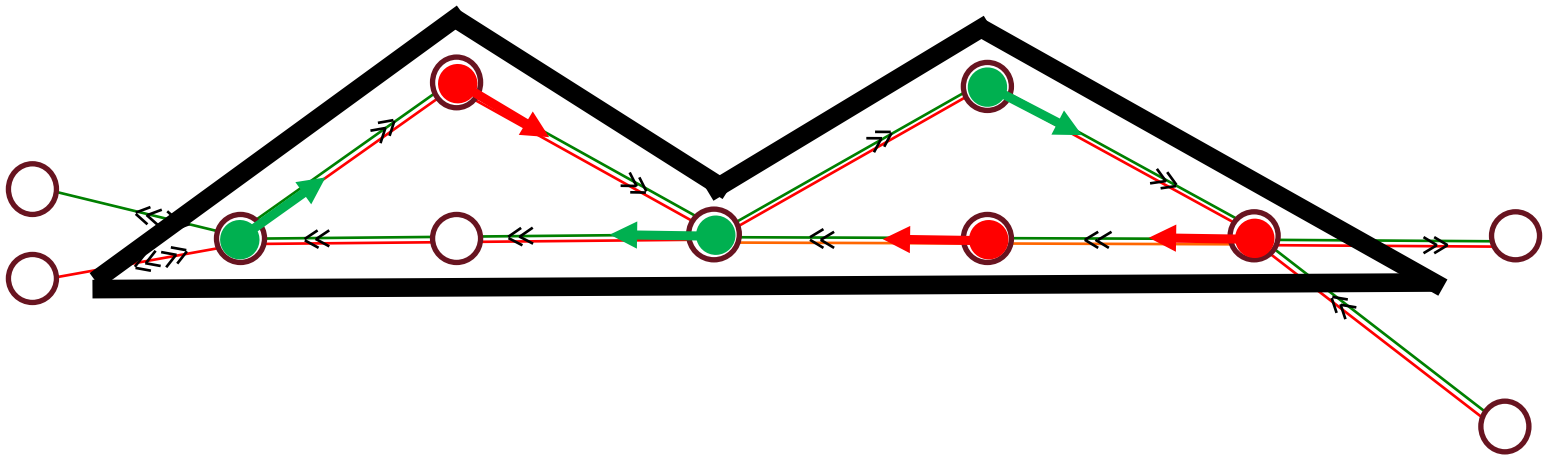
Deadlock on composite sections I



Solution:

No more than 3 itineraries booked inside this section of size 5.

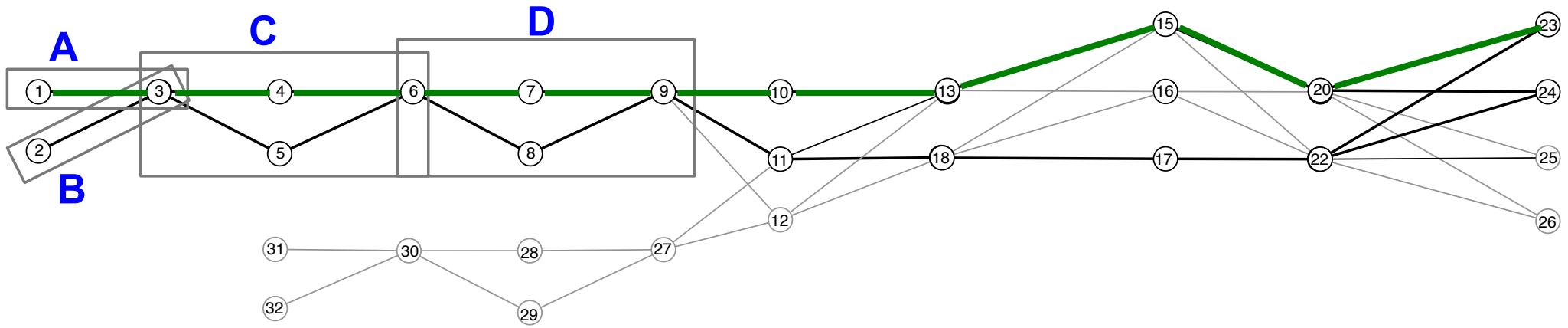
Deadlock on composite sections II



Solution:

No more than 5 itineraries booked inside this section of size 8

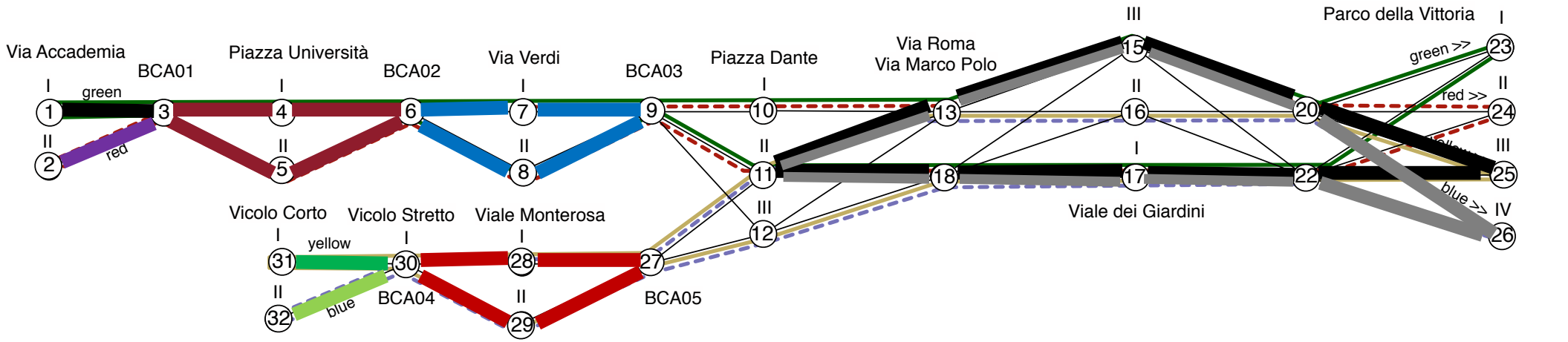
Extended missions



[1 ,3, 4, 6, 7, 9, 10, 13, 15, 20 ,23, . . .]

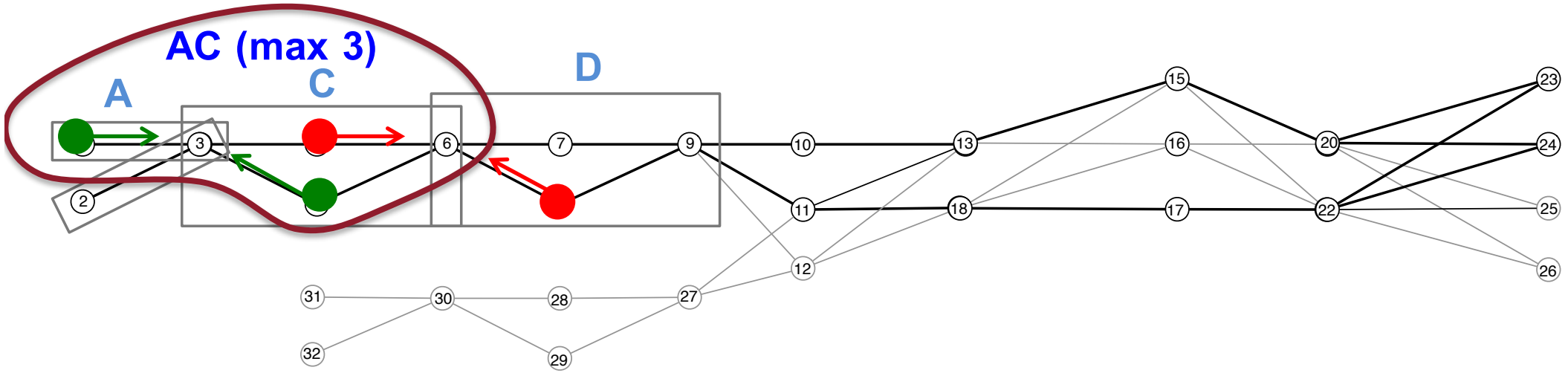
[*(A++;AC++)* 1, *([C<4];A--;C++)* 3, 4, *([D<4];C--;AC--;D++)* 6, 7, *(D--)* 9, . . .]

Discovering basic critical sections



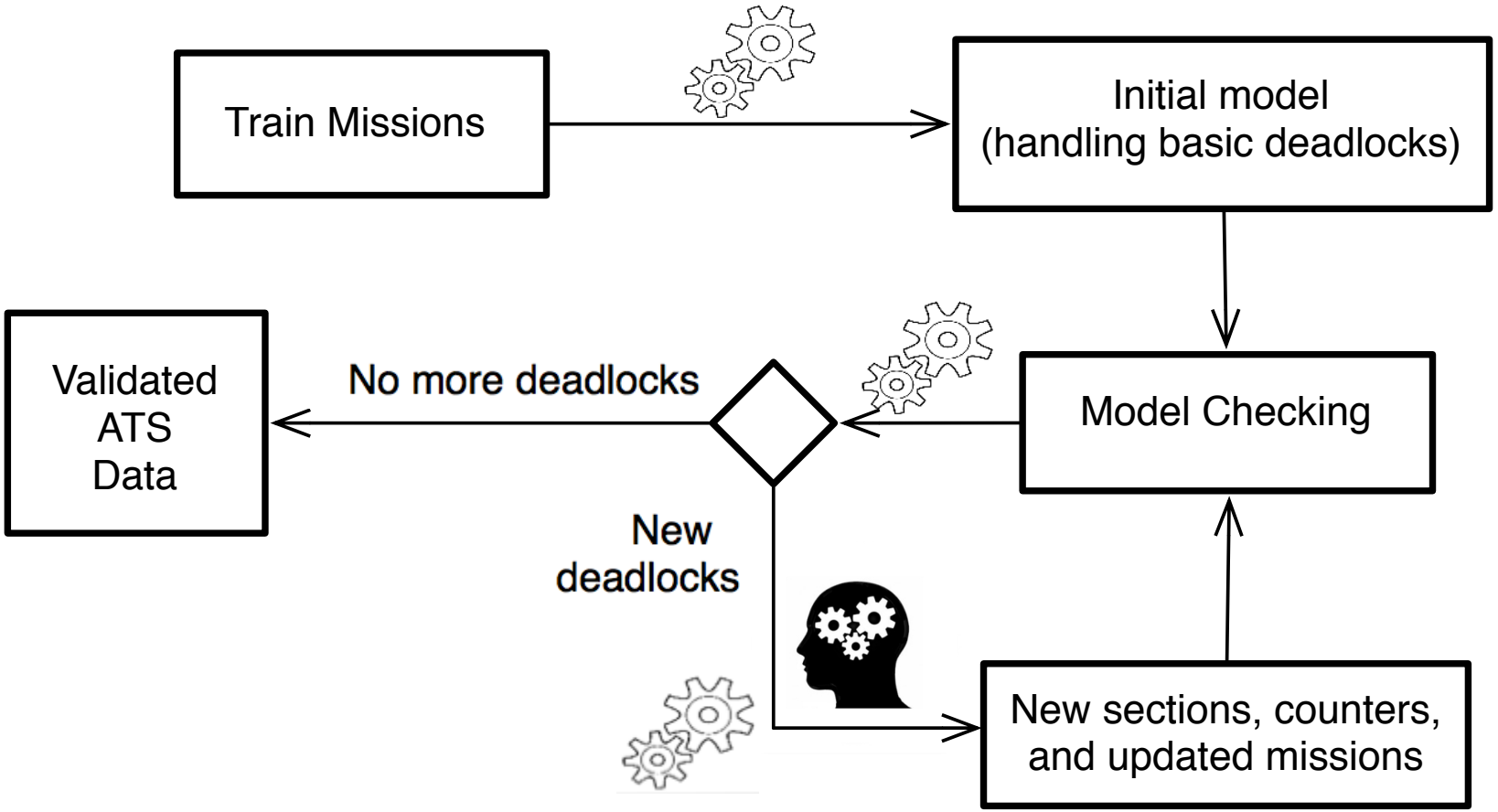
Basic critical sections (rings, bidirectional segments) can be discovered by an analysis of the possible missions.

Discovering composite critical sections



We build a **formal model** of the system and use **model checking** techniques to find **all** situations of deadlock in the composite sections.

The role of model checking

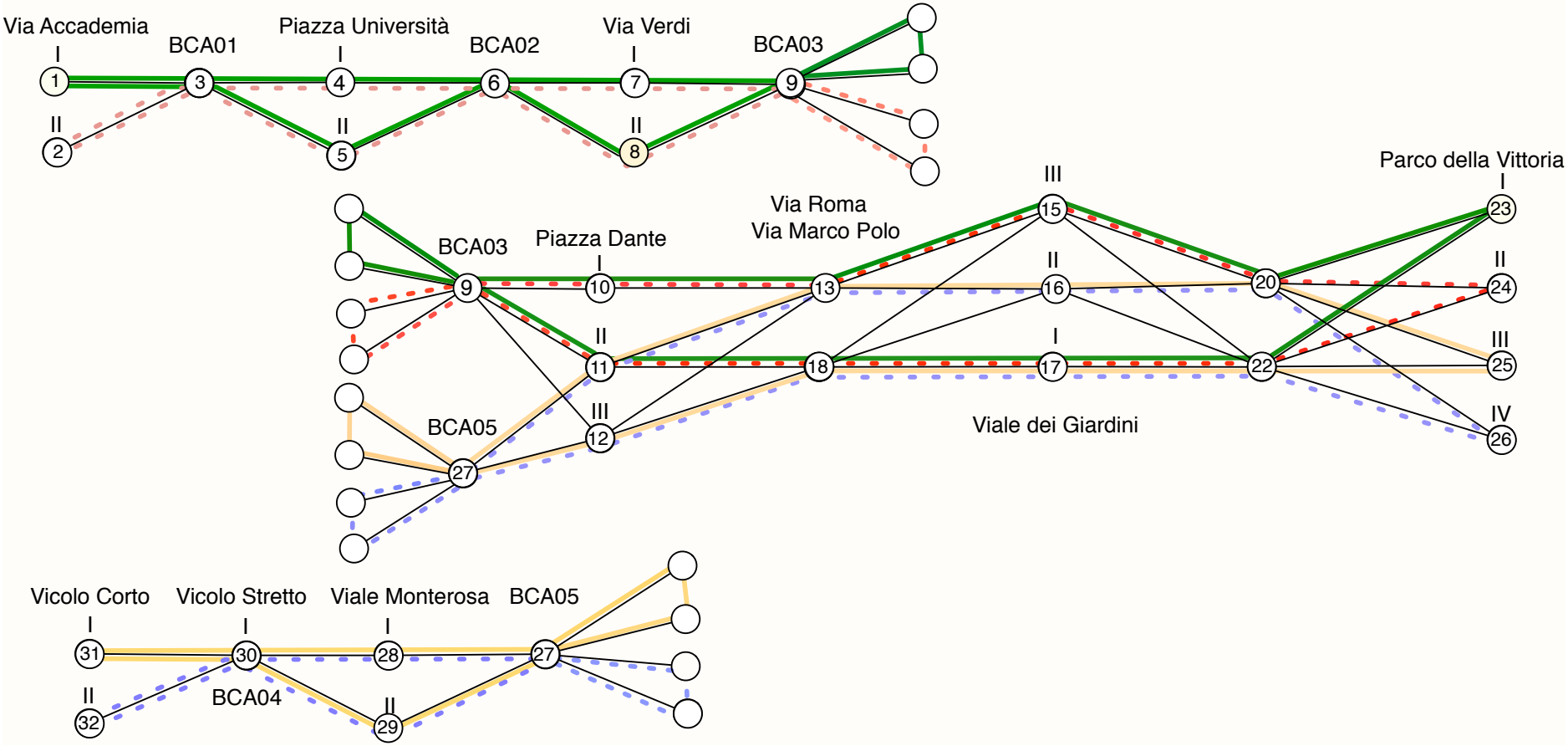


The role of model checking

In the TRACE-IT case study ATS data validation is done statically at configuration / reconfiguration time.

We have also experimented a dynamic automatic approach using a custom ad hoc model checker.

System Decomposition



References

More details on the approach to deadlock avoidance:

Mazzanti, F., Spagnolo, G.O., Della Longa, S., Ferrari, A.

Deadlock avoidance in train scheduling: A model checking approach

9th International Conference on Formal Methods for Industrial Critical Systems, FMICS 2014;
Lecture Notes in Computer Science - Volume 8718, 2014

Examples and comparisons of formal modelling and verification approaches using SPIN / SMV / UMC / MCRL2

Mazzanti, F., Ferrari, A., Spagnolo, G.O.

Experiments in Formal Modelling of a Deadlock Avoidance Algorithm for a CBTC System

T. Margaria and B. Steffen (Eds) ISoLA 2016, Part II
Lecture Notes in Computer Science - Volume 9953, 2016


ASTRail
SAtellite-based Signalling and Automation SysTems
on Railways along with Formal Method and Moving Block validation
THANK YOU!
CONTACTS
Franco Mazzanti
Senior Researcher
ISTI CNR Via Moruzzi 1, Pisa , Italy
http://fmt.isti.cnr.it/~mazzanti
Shift2Rail
This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 777561
Call identifier: H2020-S2RJU-2017
Topic: S2R-OC-IP2-01-2017 – Operational conditions of the signalling and automation systems; signalling system hazard analysis and GNSS SIS characterization along with Formal Method application in railway field
ISMB
Sirti
Ardanuy
ENAC
unife