Formal Methods and Tools: a brief introduction

Maurice H. ter Beek

FMT lab, ISTI-CNR, Pisa, Italy

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

Introduction

About me

- Senior researcher, FMT lab, ISTI–CNR, lab head since 2019
- M.Sc. (’96) and Ph.D. (‘03) degrees, Leiden University, NL
- Formal methods, model checking (tools), SPLE, SOC, team automata, railways

About me

- Senior researcher, FMT lab, ISTI–CNR, lab head since 2019
- M.Sc. (’96) and Ph.D. (‘03) degrees, Leiden University, NL
- Formal methods, model checking (tools), SPLE, SOC, team automata, railways

Consiglio Nazionale delle Ricerche

Italy's National Research Council (CNR)

- Est. 1923, full range of scientific areas, annual budget 1B€
- More than 9000 FTE (⅔ scientists), >2000 junior scientists
- Mission: perform research, training, technology transfer, promote innovation and competitiveness in industry and society, advise the government and other public bodies

Consiglio Nazionale delle Ricerche

Italy's National Research Council (CNR)

- Est. 1923, full range of scientific areas, annual budget 1B€
- More than 9000 FTE (⅔ scientists), >2000 junior scientists
- Mission: perform research, training, technology transfer, promote innovation and competitiveness in industry and society, advise the government and other public bodies
- Institute of Information Science and Technologies (ISTI), Pisa

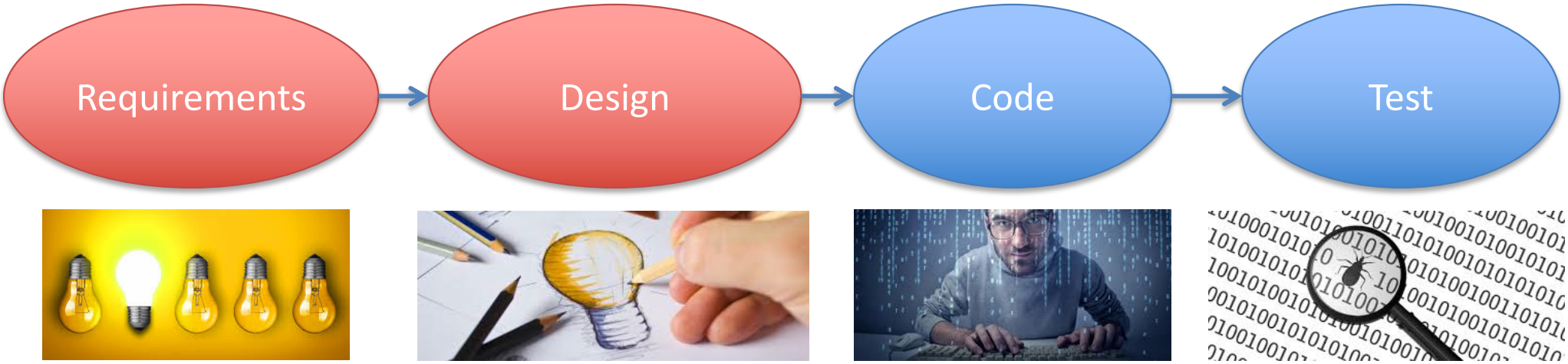
- Research campus: 123,300 m^2
  >1500 persons (±1000 CNR)

Research Infrastructures

Research infrastructures are mainly located within the Research Parks, grouping together institutes with related scientific tasks, sharing common services. The use of some large research infrastructures is also made available to researchers belonging to other scientific institutions in Italy and abroad, such as marine vessels, or other facilities settled in remote locations (i.e. Svalbard islands and Himalaya region) for environmental research.

Formal Methods and Tools (FMT)

Software Development Process



Formal Methods and Tools (FMT)

Software Development Process

Requirements → Design → Code → Test




- Model Checking
- Product Line Engineering
- Natural Language Processing




eGov

Techniques and Tools

Application Domains

Formal Methods and Tools: techniques and tools

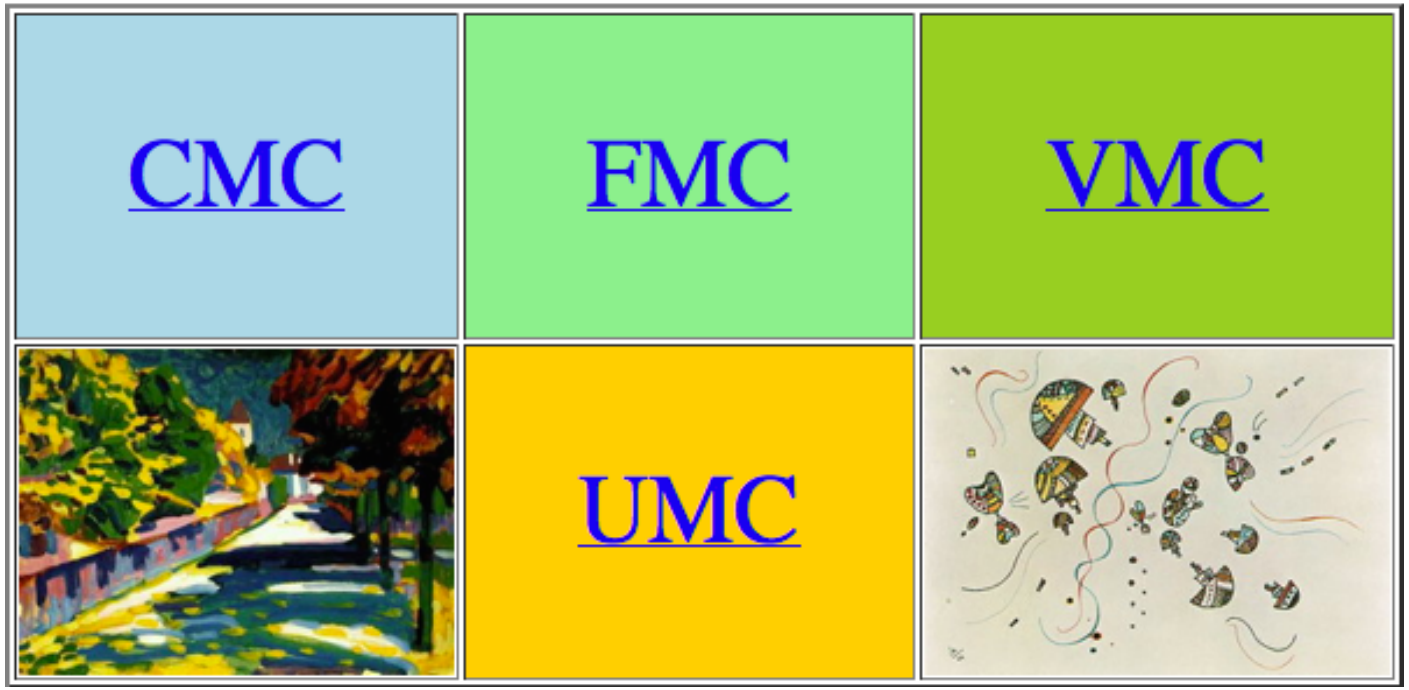
Formal Methods

"Rigorous techniques, based on mathematical foundations, for the specification and verification of software (systems)"

© 2018 Galois, Inc., USA

and Tools

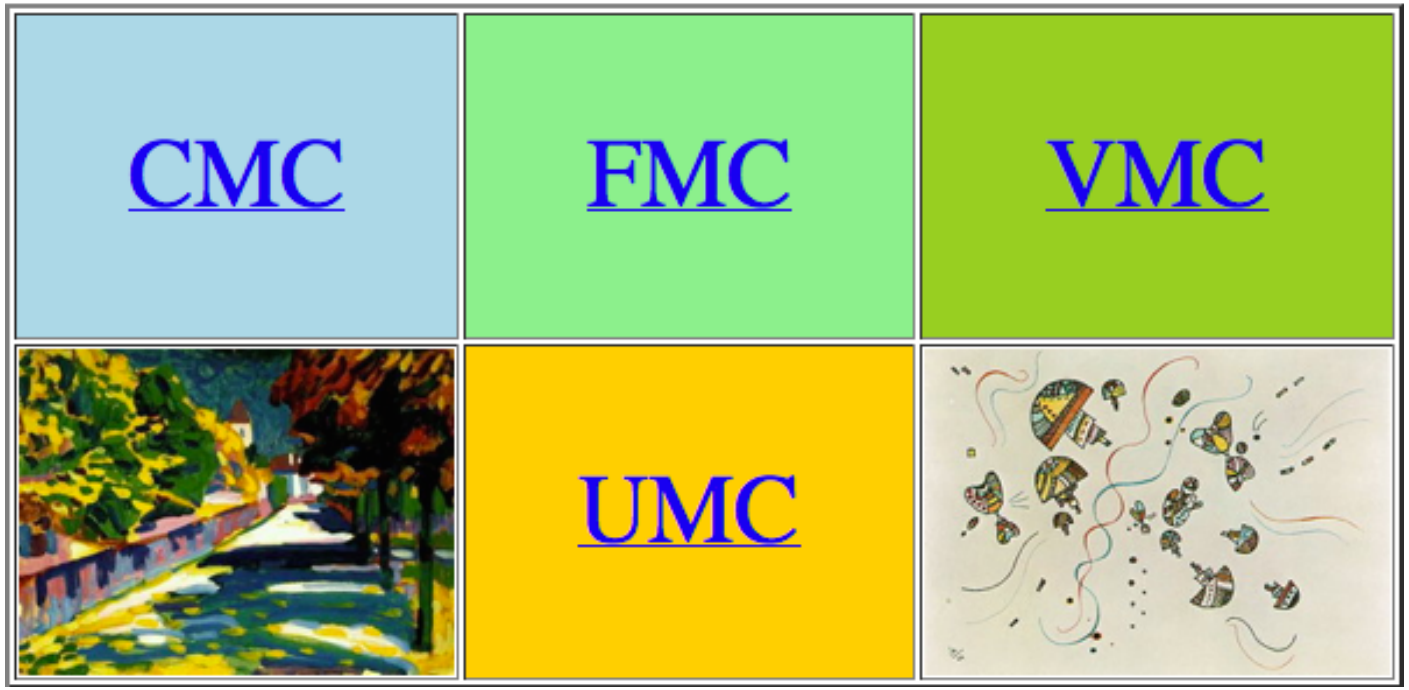
- KandISTI: family of model checkers developed by FMT for >2 decades



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

and Tools

- KandISTI: family of model checkers developed by FMT for >2 decades



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

Explicit-state on-the-fly model checking of properties in state- and action-based branching-time temporal logics
e.g. UCTL, SocL, v-ACTL

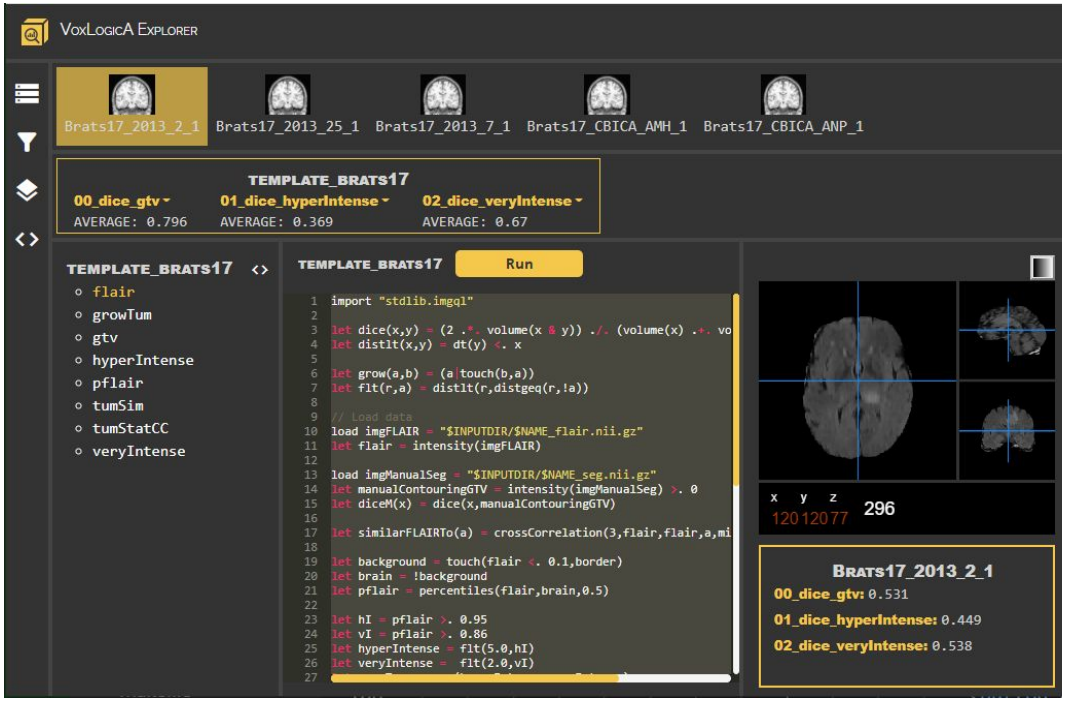
Complexity linear w.r.t. size of model and size of formula

and Tools

- QuARS: Quality Analyzer of Requirements Specification

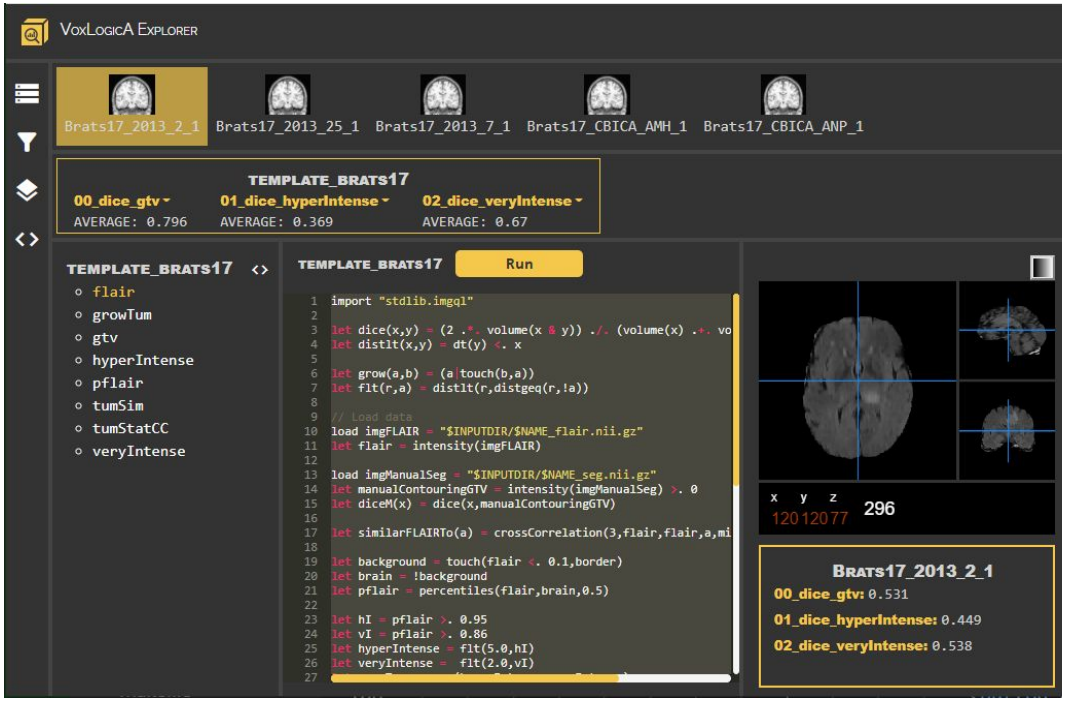
and Tools

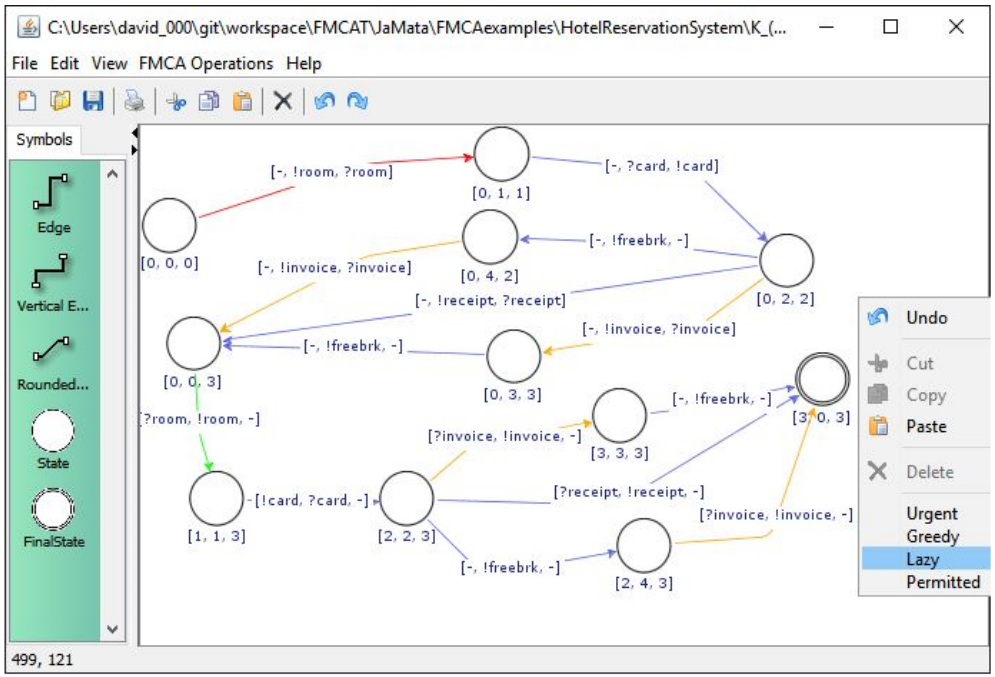
- QuARS: Quality Analyzer of Requirements Specification
- VoxLogicA / Topochecker: Spatio(-temporal) model checking and image analysis



and Tools

- QuARS: Quality Analyzer of Requirements Specification
- VoxLogicA / Topochecker: Spatio(-temporal) model checking and image analysis
- Contract Automata Tool: Controller synthesis for service contracts





Formal Methods and Tools

- Process algebras and automata (probabilistic, stochastic, …)
- Temporal and spatial logics and model-checking tools
- KandISTI (UMC, CMC, FMC, VMC), QuARS, VoxLogicA, CAT, …
- Qualitative and quantitative (statistical model checking) formal analysis

Formal Methods and Tools

- Process algebras and automata (probabilistic, stochastic, …)
- Temporal and spatial logics and model-checking tools
- KandISTI (UMC, CMC, FMC, VMC), QuARS, VoxLogicA, CAT, …
- Qualitative and quantitative (statistical model checking) formal analysis

Software Engineering at large:

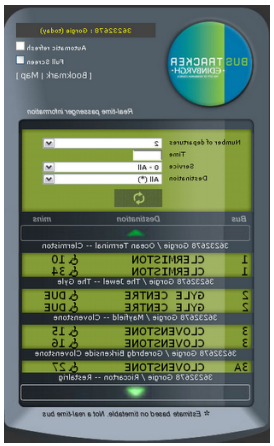
- Natural Language Processing applications
- Requirements Engineering
- Empirical Software Engineering
- …

Formal Methods and Tools: application domains

(recent project experiences)

FUNDAMENTALS OF COLLECTIVE ADAPTIVE SYSTEMS

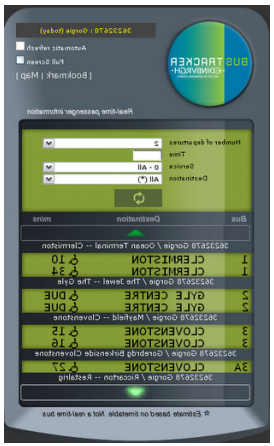
CAS for a smart society: smart urban transport, smart grids



Objective: support fair and efficient resource management in systems of heterogeneous components with competing goals

FUNDAMENTALS OF COLLECTIVE ADAPTIVE SYSTEMS

CAS for a smart society: smart urban transport, smart grids



Objective: support fair and efficient resource management in systems of heterogeneous components with competing goals

With bike-sharing systems as case study, FMT focussed on:

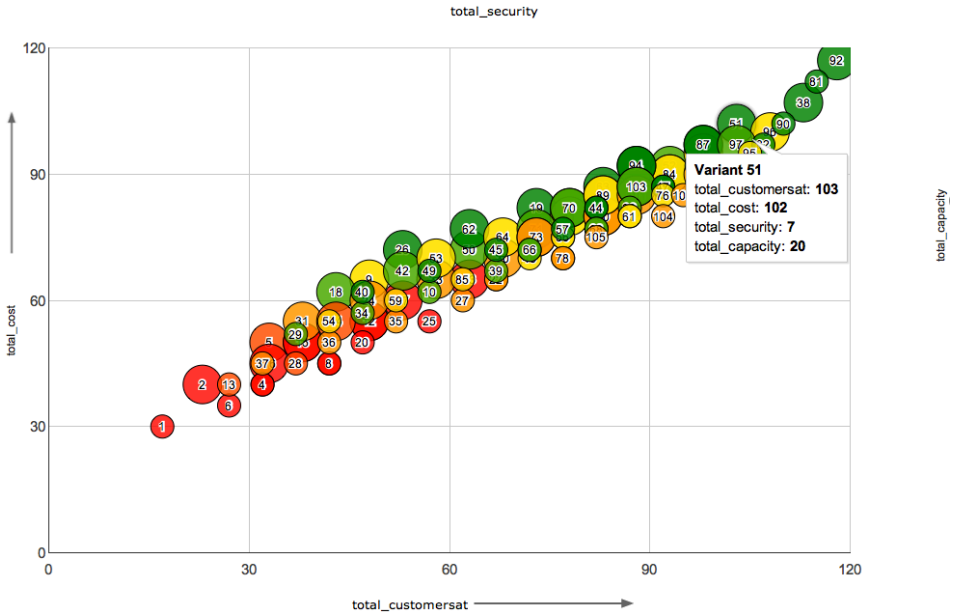
- Scalable formal verification approaches for CAS
- Quantitative business models and product lines

Variability Analysis of Pisa's Bike-sharing System

Aim: systematic evaluation of options for improvement (i.e. costs/benefits) *before* actually implementing them

Variability Analysis of Pisa's Bike-sharing System

Aim: systematic evaluation of options for improvement (i.e. costs/benefits) *before* actually implementing them

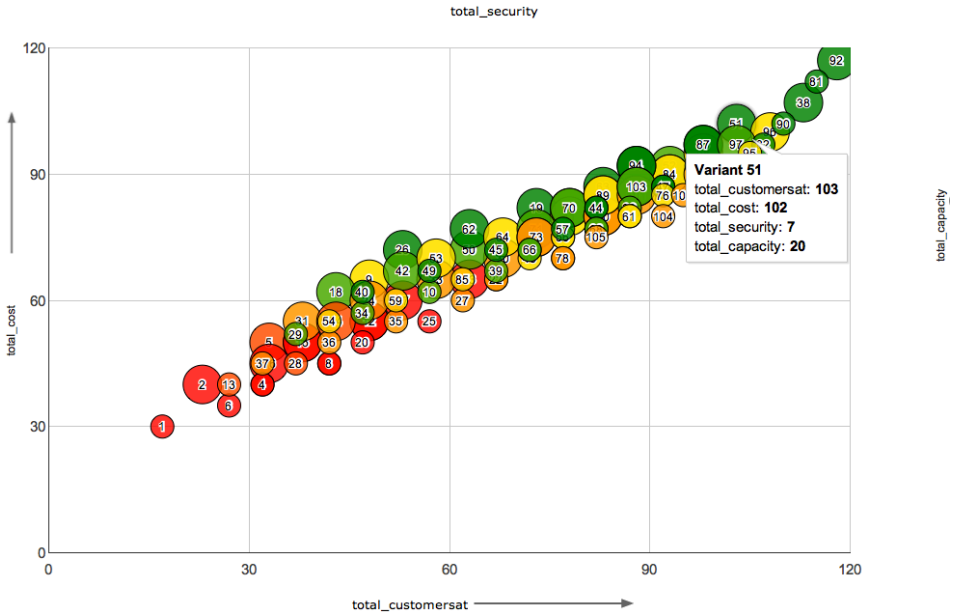


MOO attributed feature models with Clafer [Czarnecki et al.]:

- Compare system configurations w.r.t. various quality dimensions, select the most desirable variant (possibly resolving trade-offs) and understand the impact of re-configurations on a variant's quality dimensions

Variability Analysis of Pisa's Bike-sharing System

Aim: systematic evaluation of options for improvement (i.e. costs/benefits) *before* actually implementing them

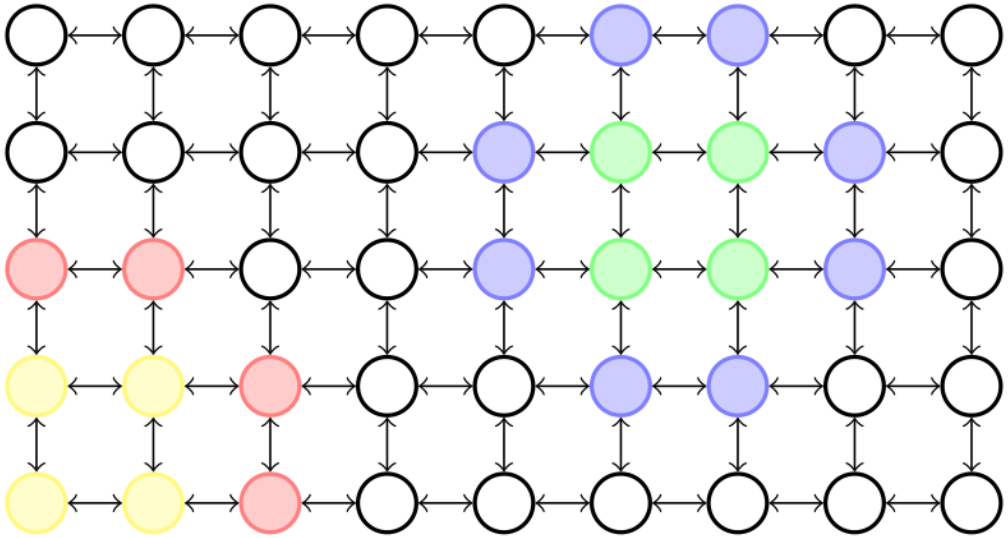


Mean field model checking with FlyFast:

- If we augment the capacity of some stations (e.g. in centre), then how does this effect the occupation level of all stations?
- If we add a station between the centre and a little used peripheral station, does the latter's usage frequency increase?

Statistical Spatio-temporal Model Checking

Reachability properties in graphs (discretised physical space)



$$
\begin{array}{lcll}
\Phi & ::= & p & [\textsc{Atomic proposition}] \\
 & | & \top & [\textsc{True}] \\
 & | & \neg\Phi & [\textsc{Not}] \\
 & | & \Phi \wedge \Phi & [\textsc{And}] \\
 & | & \mathcal{N}\Phi & [\textsc{Near}] \\
 & | & \Phi\,\mathcal{S}\,\Phi & [\textsc{Surrounded}]
\end{array}
$$

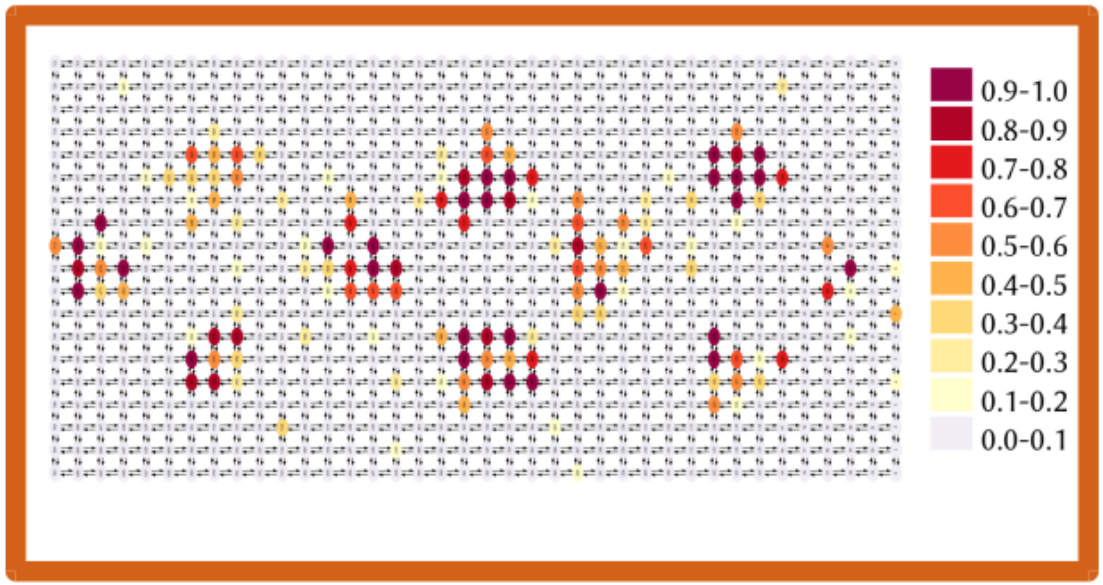
Derived operators, like interior: $\mathcal{I}\Phi = \neg\mathcal{N}\neg\Phi$

All red and yellow points satisfy: $\mathcal{N}\,yellow$
One yellow point satisfies: $\mathcal{I}\,yellow$
No points satisfy: $\mathcal{I}\,green$
Green points satisfy: $green\,\mathcal{S}\,blue$

LMCS, STTT, ISoLA

Statistical Spatio-temporal Model Checking

Reachability properties in graphs (discretised physical space)



$$
\begin{array}{lcll}
\Phi & ::= & p & [\textsc{Atomic proposition}] \\
 & | & \top & [\textsc{True}] \\
 & | & \neg\Phi & [\textsc{Not}] \\
 & | & \Phi \wedge \Phi & [\textsc{And}] \\
 & | & \mathcal{N}\Phi & [\textsc{Near}] \\
 & | & \Phi\,\mathcal{S}\,\Phi & [\textsc{Surrounded}]
\end{array}
$$

Derived operators, like interior: $\mathcal{I}\Phi = \neg\mathcal{N}\neg\Phi$

Spot congestion in bike-sharing system:

full = [vacantPlaces == 0]

cluster = I full

eventuallyCluster = EF cluster

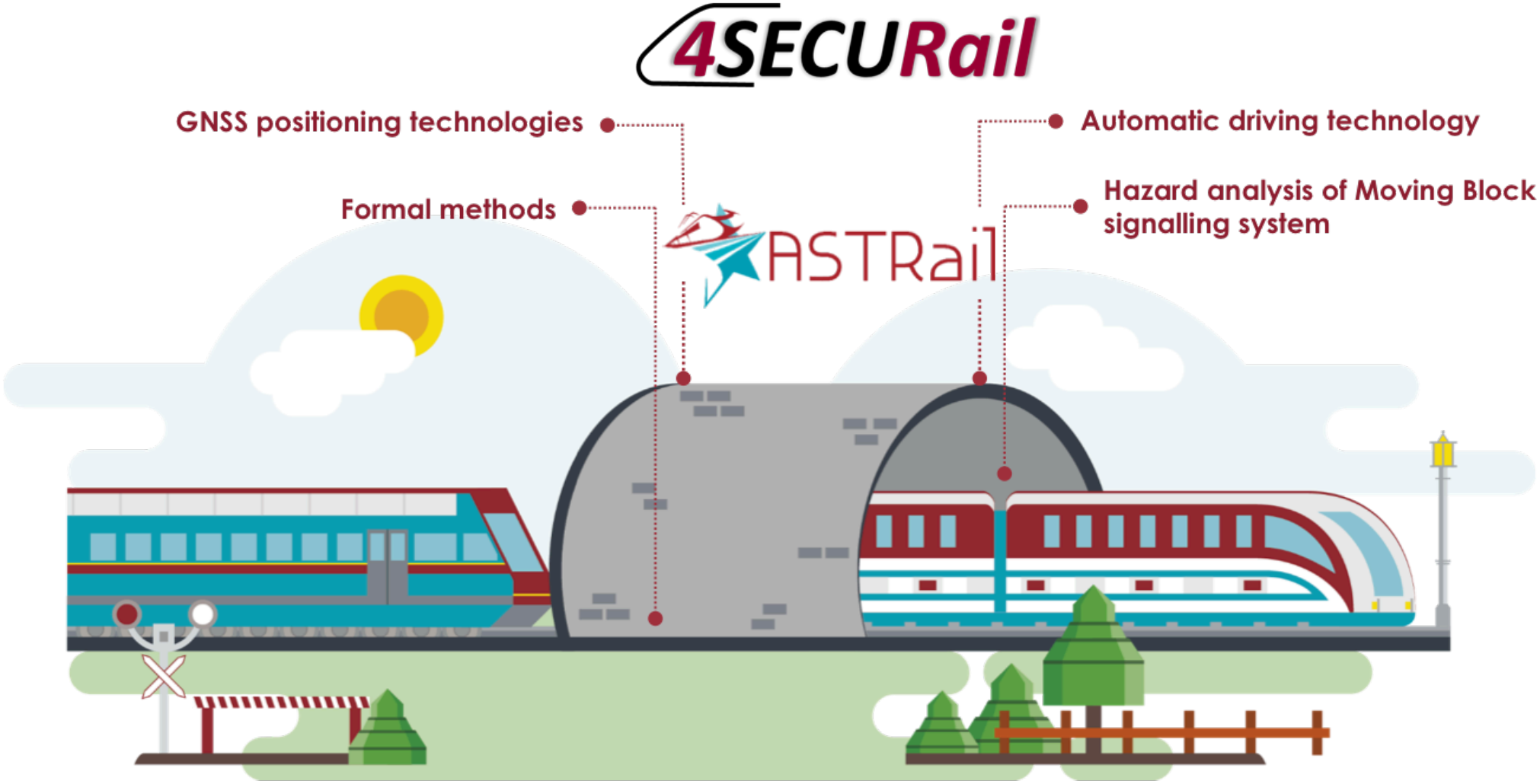
LMCS, STTT, ISoLA

H2020 Shift2Rail Initiative: 920M€ (2014–20)

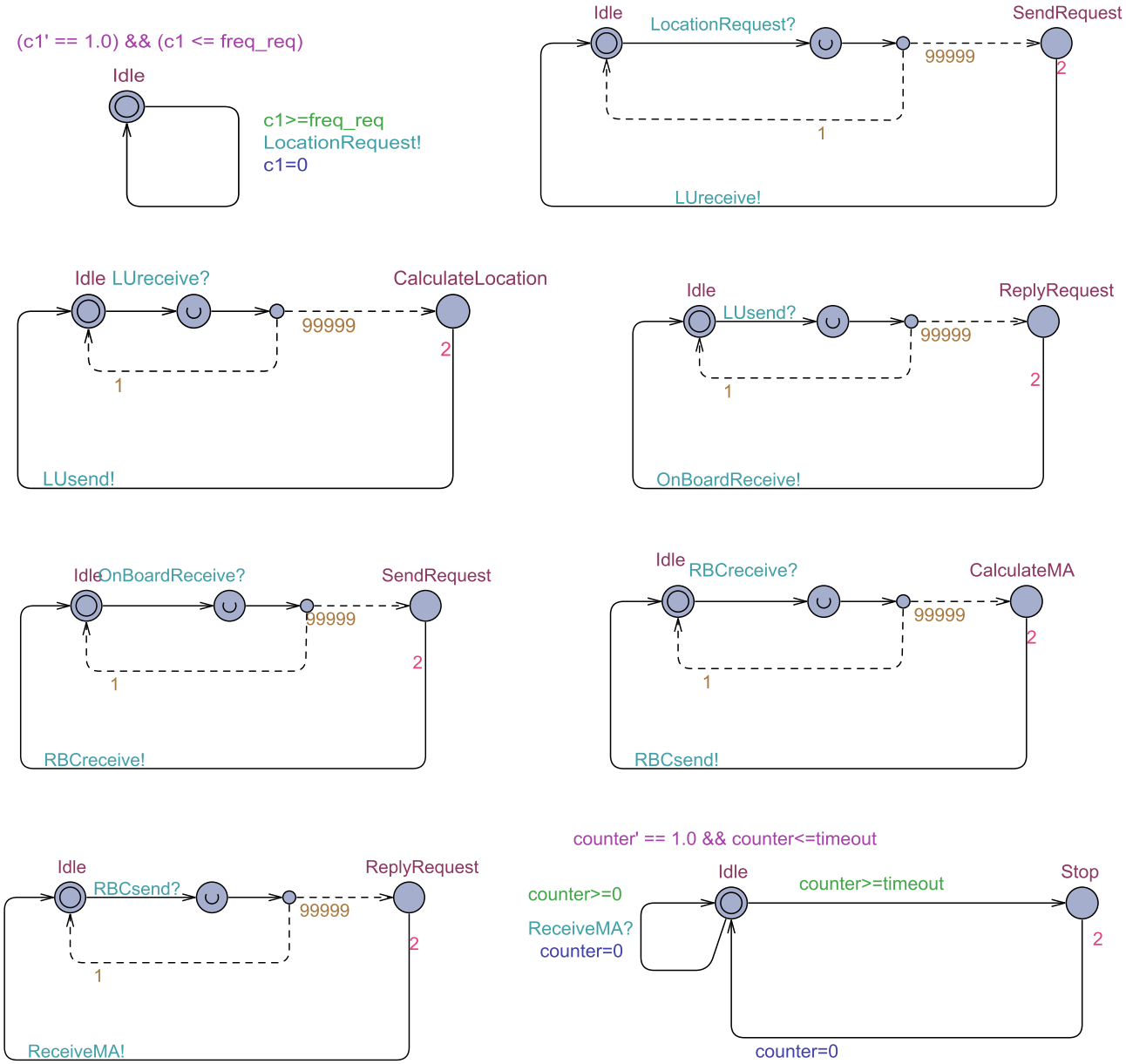
“Formal methods are fundamental for safe and reliable technological advances to increase the competitiveness of the European rail industry”

H2020 Shift2Rail Initiative: 920M€ (2014–20)

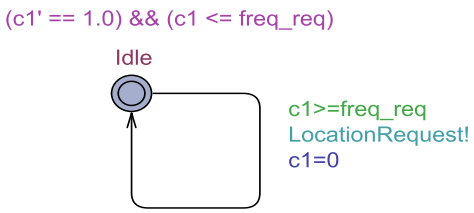
"Formal methods are fundamental for safe and reliable technological advances to increase the competitiveness of the European rail industry"

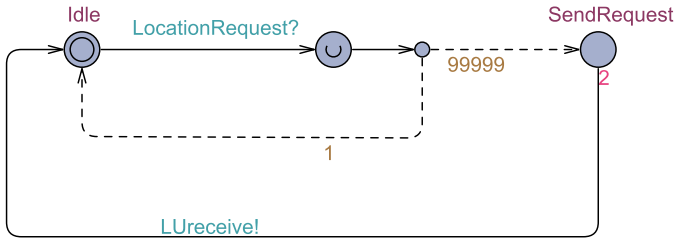


Statistical Model Checking of a Moving Block Railway Signalling Scenario with Uppaal SMC



Statistical Model Checking of a Moving Block Railway Signalling Scenario with Uppaal SMC

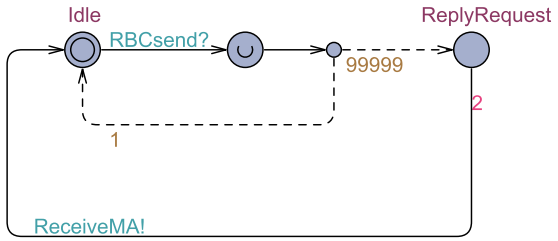


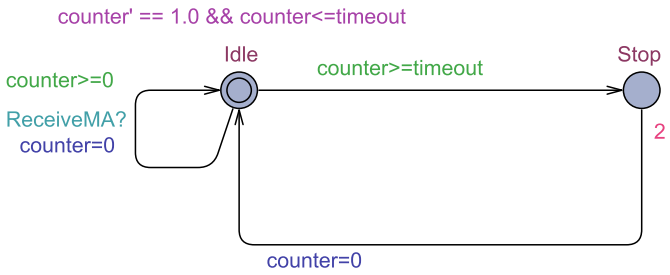


Probability that train enters safe state Stop upon timeout:

$$\mathbb{P}_M(\Diamond_{\leq(\texttt{timeout})}\,\texttt{Controlling.Stop})$$

Uppaal SMC [Larsen et al.] reports that this probability is in the interval [0,9.99994e-005], with confidence 0.995, obtained from 59912 runs in ±5 minutes (*M* is the model)





Unione Europea
Fondo Europeo di Sviluppo Regionale

Regione Toscana

2014 2020 POR CreO
PROGRAMMA OPERATIVO REGIONALE
CRESCITA e OCCUPAZIONE

Renew the role of railway stations in the future's smart cities

Unione Europea
Fondo Europeo di Sviluppo Regionale

Regione Toscana

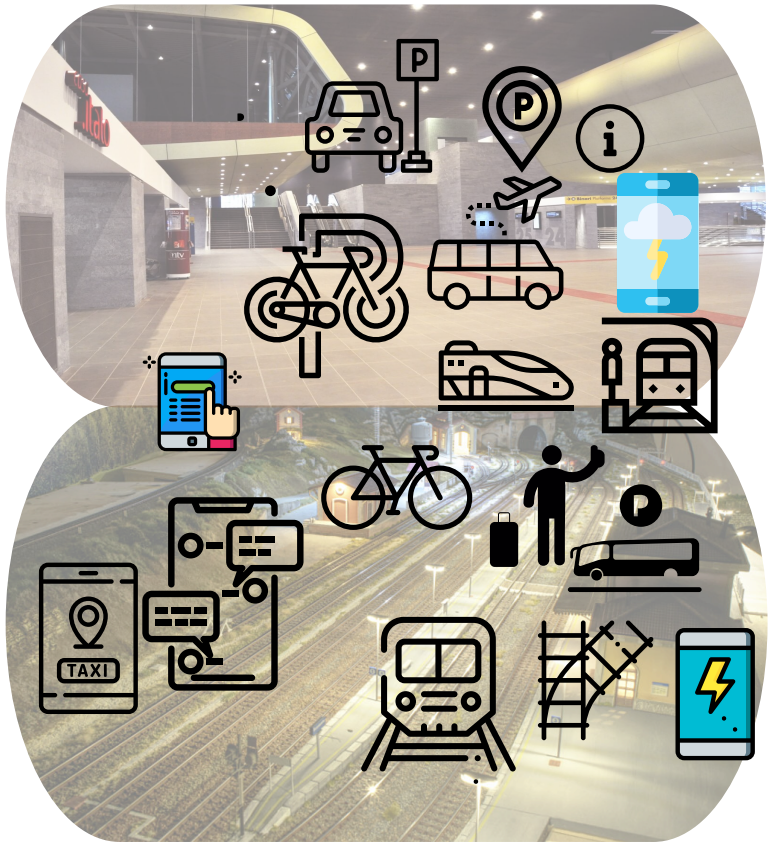
2014 2020 POR CreO
PROGRAMMA OPERATIVO REGIONALE
CRESCITA e OCCUPAZIONE

StingRay

Renew the role of railway stations in the future's smart cities

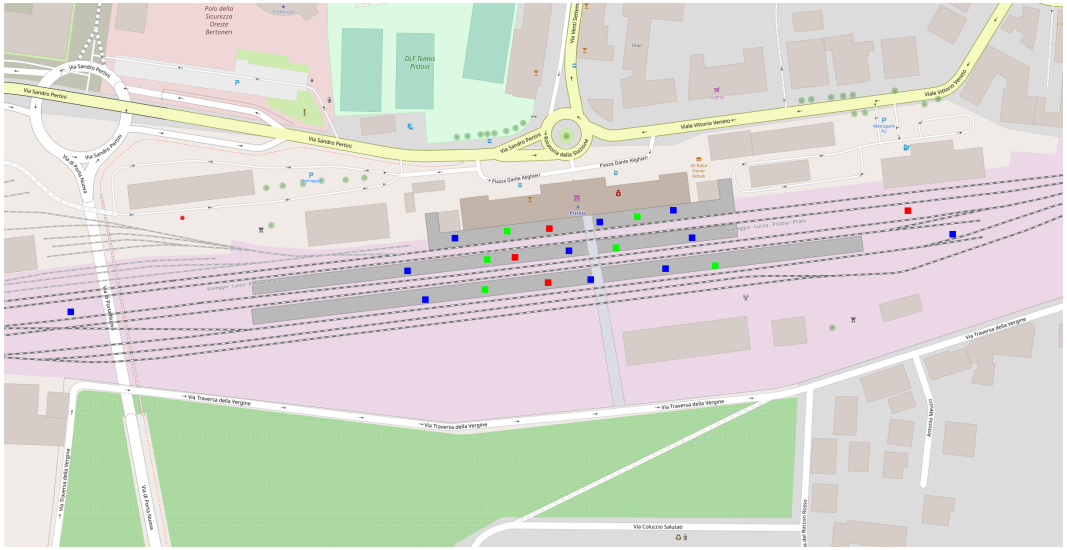
Revisit station communication infrastructure, integrating power line and wireless technologies in order to:

- Realize LAN network over station plants
- Implement remote monitoring and control of the station equipment
- Create value-added services for both customers and staff, such as connectivity, energy management, environmental surveying, video surveillance, fault prediction, and infomobility



Spatial Model Checking for Smart Stations

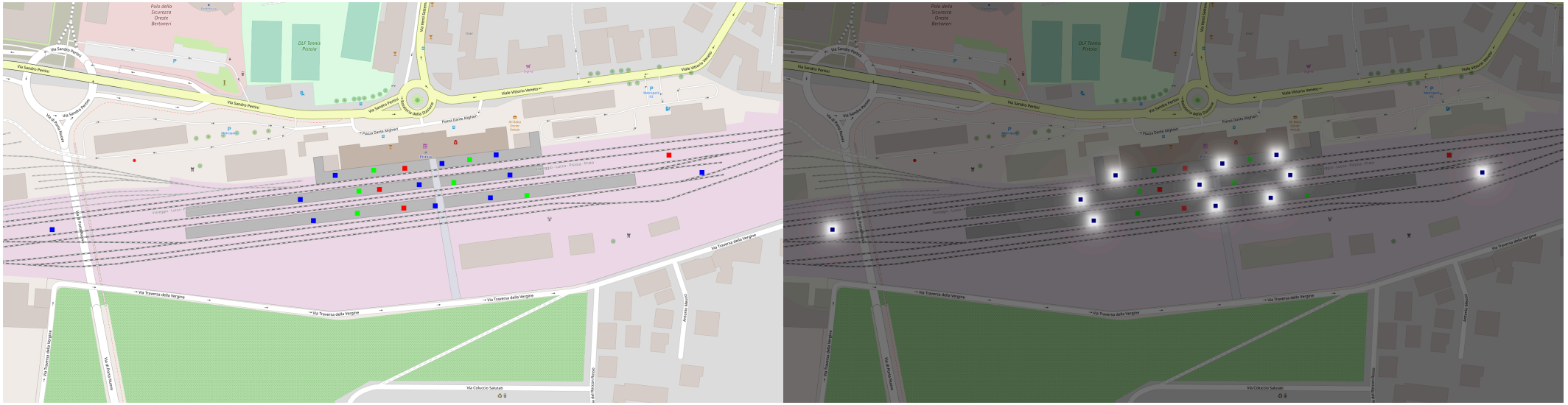
Aim: identify poorly illuminated platform areas of a station




```
let platform = grow(grow(platformSeed,platformArea),cmad|madill)
let attenuation = 1 ./ (1 .+ (0.01 .* dt(madill)) + (0.001 .* (dt(madill)*dt(madill))))
let threshold = attenuation >. 0.3
let nonIllumPlatform = platform \ threshold
```

Spatial Model Checking for Smart Stations

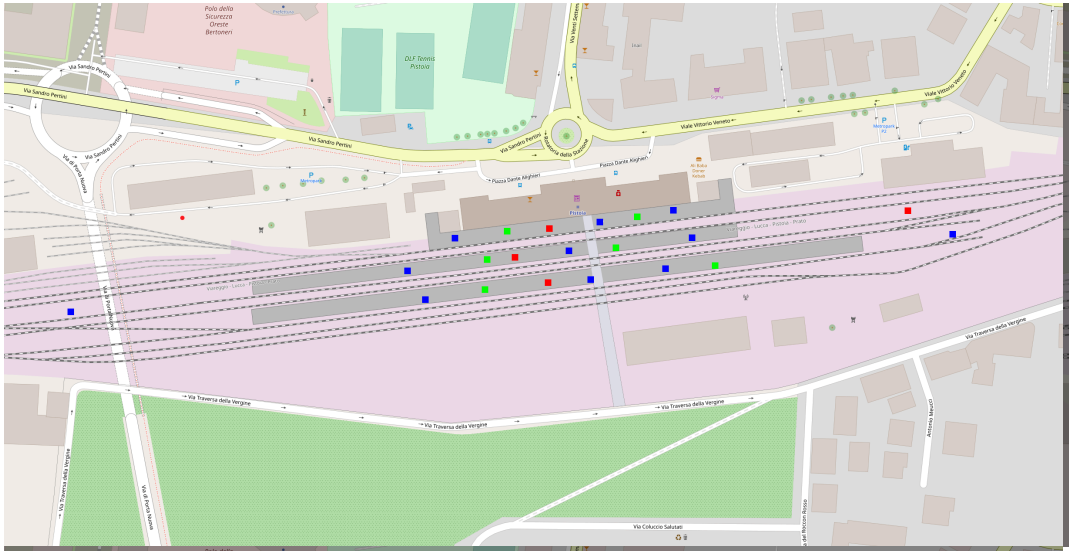
Aim: identify poorly illuminated platform areas of a station

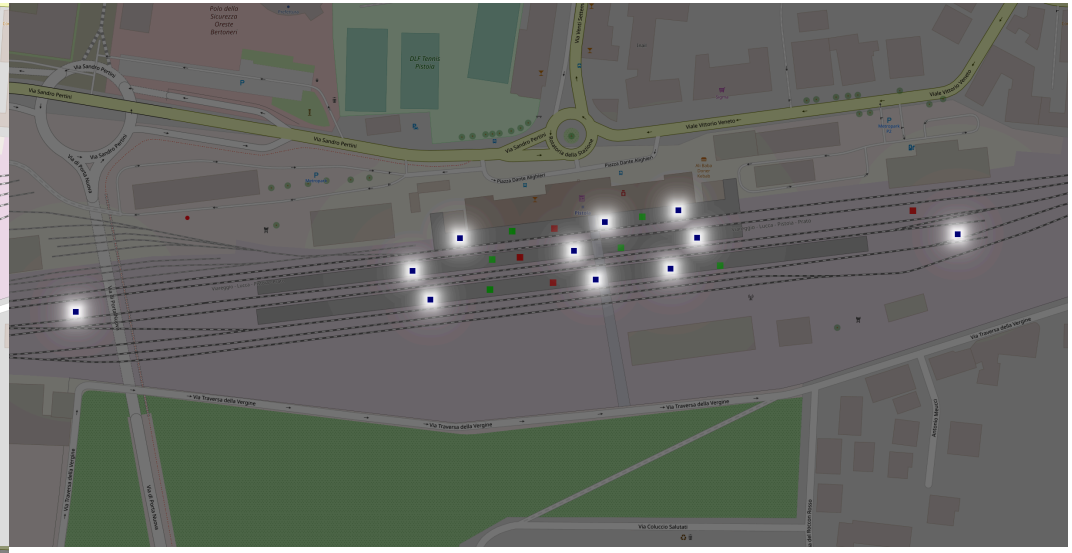


```
let platform = grow(grow(platformSeed,platformArea),cmad|madill)
let attenuation = 1 ./ (1 .+ (0.01 .* dt(madill)) + (0.001 .* (dt(madill)*dt(madill))))
let threshold = attenuation >. 0.3
let nonIllumPlatform = platform \ threshold
```

Spatial Model Checking for Smart Stations

Aim: identify poorly illuminated platform areas of a station

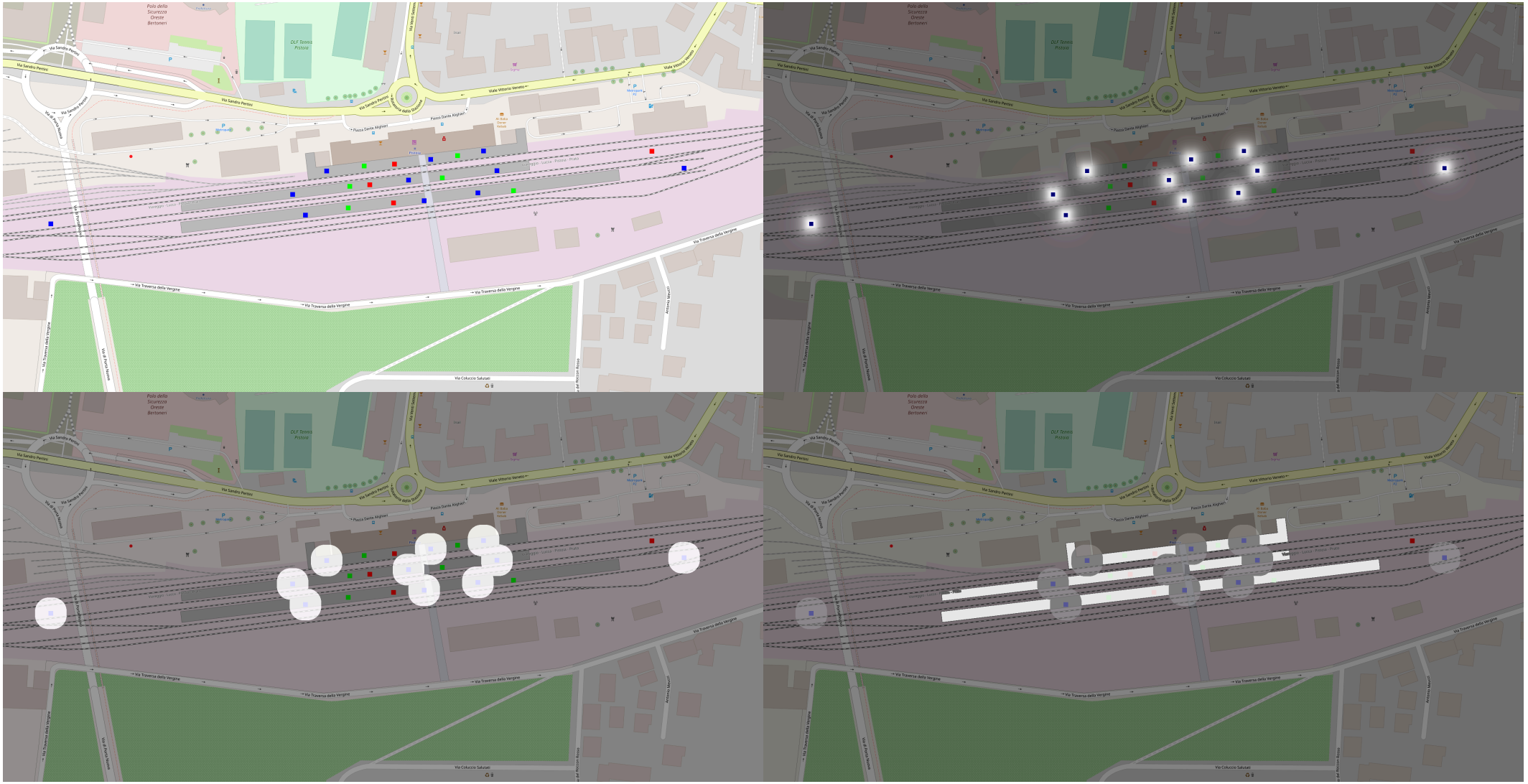




```
let platform = grow(grow(platformSeed,platformArea),cmad|madill)
let attenuation = 1 ./ (1 .+ (0.01 .* dt(madill)) + (0.001 .* (dt(madill)*dt(madill))))
let threshold = attenuation >. 0.3
let nonIllumPlatform = platform \ threshold
```

Spatial Model Checking for Smart Stations

Aim: identify poorly illuminated platform areas of a station



```
let platform = grow(grow(platformSeed,platformArea),cmad|madill)
let attenuation = 1 ./ (1 .+ (0.01 .* dt(madill)) + (0.001 .* (dt(madill)*dt(madill))))
let threshold = attenuation >. 0.3
let nonIllumPlatform = platform \ threshold
```