Moco, Falla y Fallutada:
Los supervillanos del universo SC*

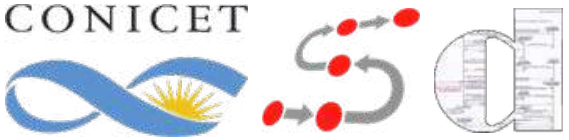
(* Sistemas Confiables)

Pedro R. D'Argenio

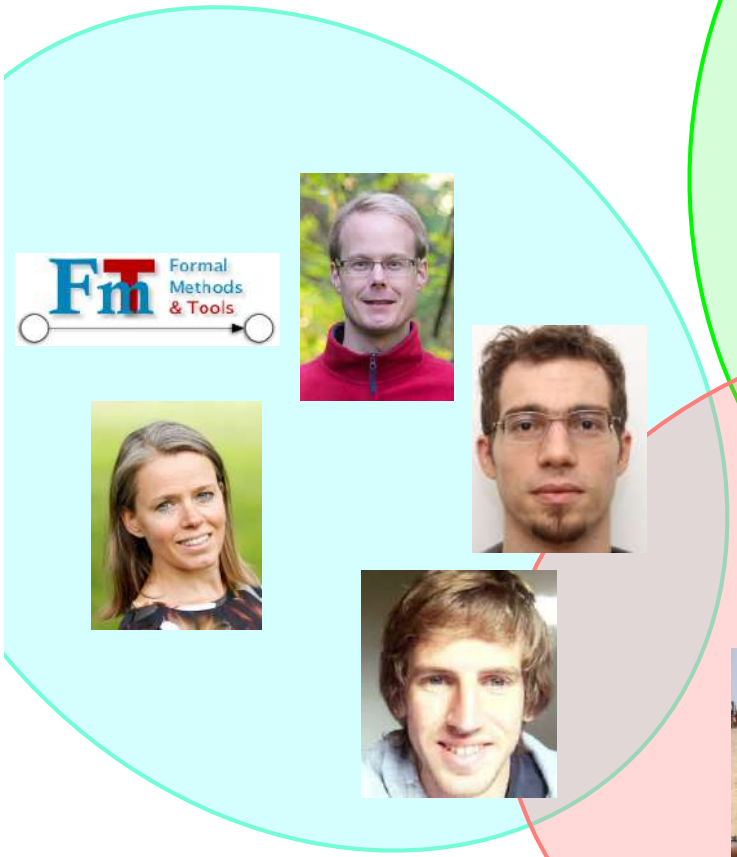
Grupo de Sistemas Confiables

Universidad Nacional de Córdoba – CONICET (AR)

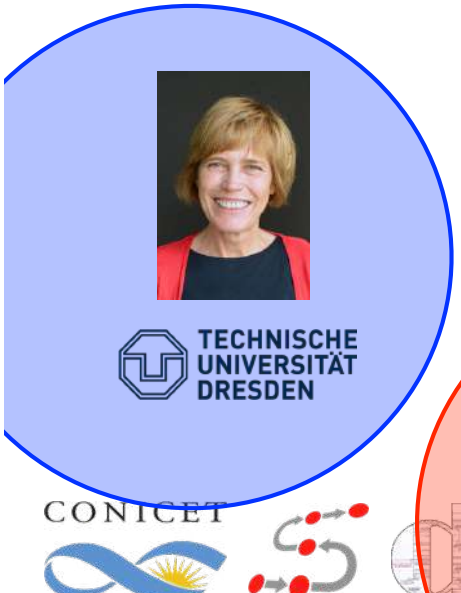
Saarland University (DE)



Mes de la Ciencia 2019 - FAMAF








Formal
Methods
& Tools
UNRC
TECHNISCHE
UNIVERSITÄT
DRESDEN
Inria
institute
IMdea
software
RWTH AACHEN
UNIVERSITY
CONICET
UNC
UNIVERSITÄT
DES
SAARLANDES

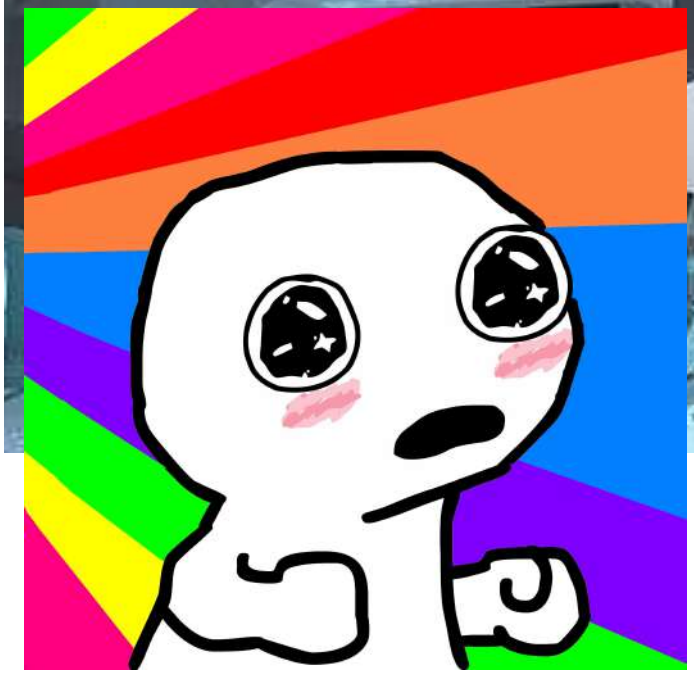
El software parece hacer maravillas…

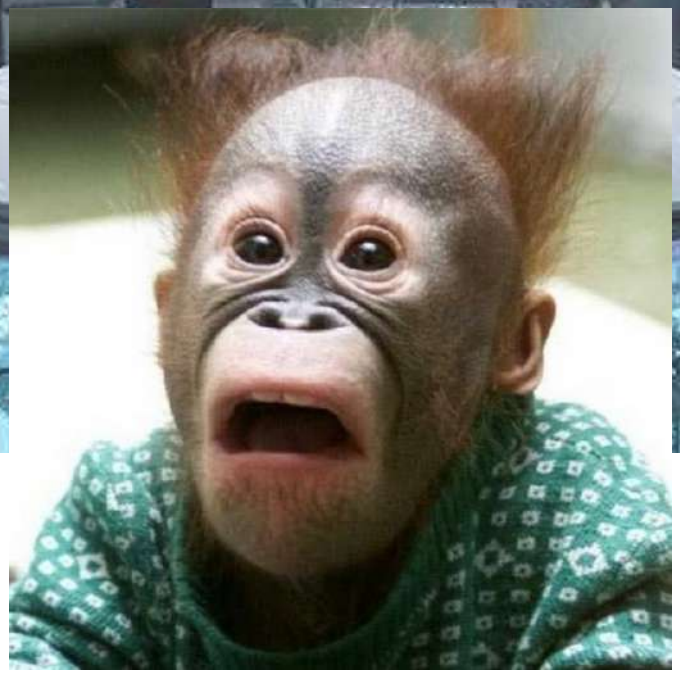
CONICET

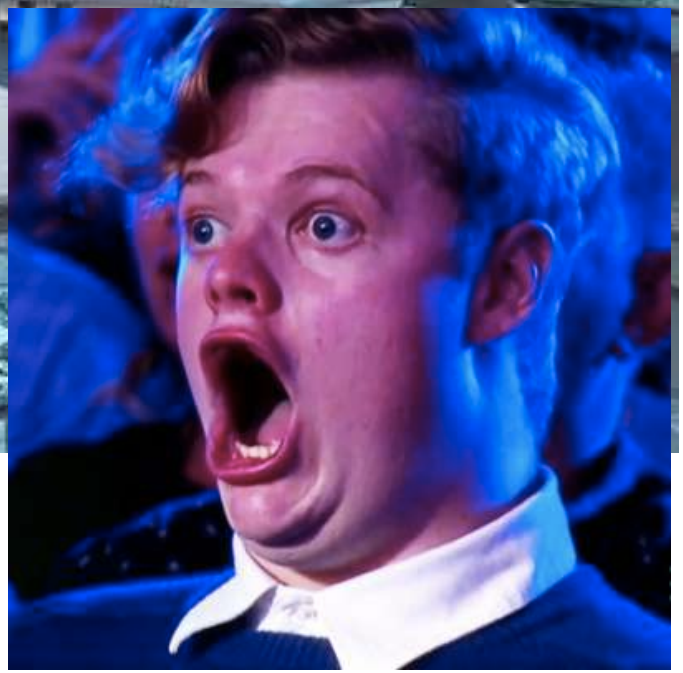
UNC

UNIVERSITÄT DES SAARLANDES

El software parece hacer maravillas…







CONICET

UNC

UNIVERSITÄT DES SAARLANDES

… pero debajo de esa cáscara de maravilla
nos encontramos con una pila de …

CONICET

UNC

UNIVERSITÄT DES SAARLANDES

¿De donde sale toda esa porquería?

- Errores en el desarrollo del software
- Fallas externas al software pero que son parte del sistema (y son mal atendidas)
- Programación malintencionada

¿De donde sale toda esa porquería?

- Errores en el desarrollo del software

Bugs

- Fallas externas al software pero que son parte del sistema (y son mal atendidas)

- Programación malintencionada

¿De donde sale toda esa porquería?

- Errores en el desarrollo del software

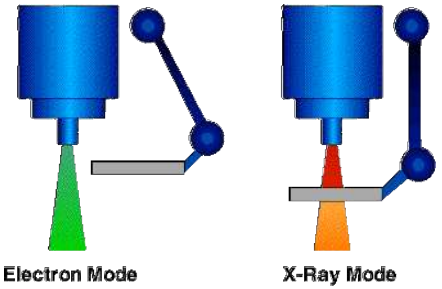
- Fallas externas al software pero que son parte del sistema (y son mal atendidas)

- Programación malintencionada

Mocos famosos

Pentium:
FDIV

Ariane 5:
64 bits fp
vs 16 bits int



Therac-25:
Condición de
carrera

Mars Climate
Orbiter:
Métrico vs Imperial

Northeast blackout
en 2003:
Condición de
carrera

Heartbleed:
Integridad/Confidencialidad

CONICET

UNC

UNIVERSITÄT
DES
SAARLANDES

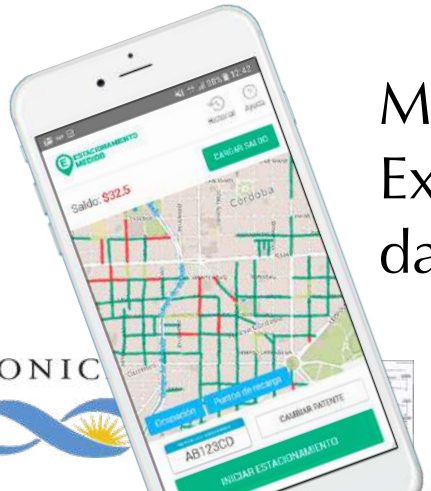
Más mocos

911 blackout:
MAX value
reached

Nest Thermostat:
Drenado de
batería

Nissan airbag:
Sensado
incorrecto

Boeing 737 MAX 8:
Sensado incorrecto



Movypark:
Exposición de
dato personales

Tesla/Uber/Google
self-driving car:
aprendizaje con
limitaciones??

CONIC

UNC

UNIVERSITÄT
DES
SAARLANDES

El problema de la corrección

$$Sistema \models Propiedad$$

Usualmente una abstracción que describe su comportamiento

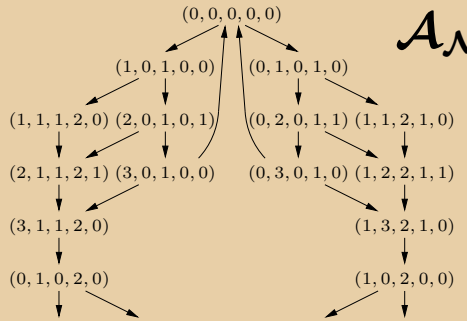
Describe lo que se espera del sistema (el criterio de corrección)

Model Checking

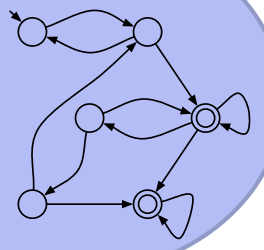
$\mathcal{M}$

```
int y1 = 0;
int y2 = 0;
short in_critical = 0;

active proctype process_1() {
  do
  :: true ->
0:      y1 = y2+1;
1:      ((y2==0) || (y1<=y2));
        in_critical++;
2:      in_critical--;
3:      y1 = 0;
  od
}

active proctype process_2() {
  do
  :: true ->
0:      y2 = y1+1;
1:      ((y1==0) || (y2<y1));
        in_critical++;
2:      in_critical--;
3:      y2 = 0;
  od
}
```

$\mathcal{A}_{\mathcal{M}}$



$\mathcal{A}_{\neg\phi}$

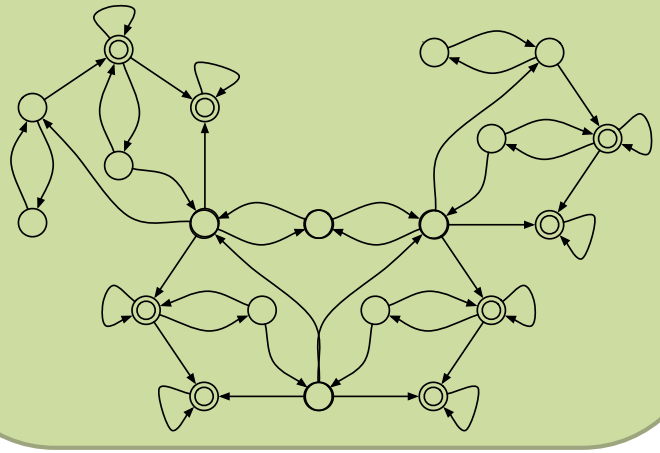


ϕ : $\Box\Diamond crit_1 \wedge \Box\Diamond crit_2$

¿ $\mathcal{M} \models \phi$?

El problema se reduce a análisis de grafos

¿ $\mathcal{A}_{\mathcal{M}} \cap \mathcal{A}_{\neg\phi} = \emptyset$?



Limitaciones del Model Checking

- Muchos algoritmos proponen (mejores) soluciones utilizando aleatoriedad.
  - Leader Election Protocol en IEEE 1394 “Firewire”
  - Binary Exponential Backoff en IEEE 802.3 “Ethernet”

- Muchas veces no se puede establecer corrección con una lógica bivaluada. Sin embargo la validez de la propiedad puede cuantificarse probabilísticamente.
  - Bounded Retransmission Protocol en Philips RC6
  - Binary Exponential Backoff en IEEE 802.3 “Ethernet”

Model Checking Cuantitativo

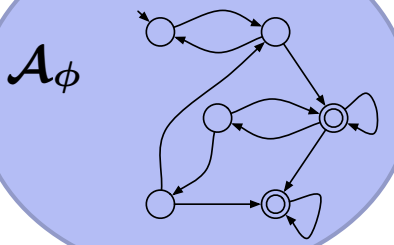
$¿\mathcal{M} \models \phi?$

$\mathcal{M}$

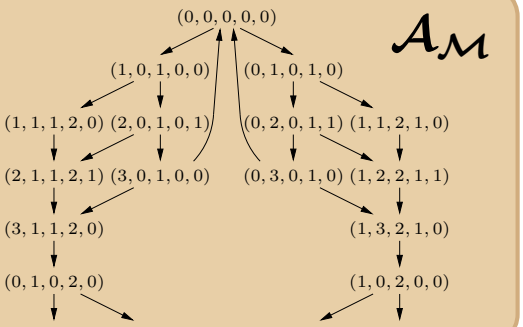
```
int y1 = 0;
int y2 = 0;
short in_critical = 0;

active proctype process_1() {
  do
  :: true ->
0:      y1 = y2+1;
1:      ((y2==0) || (y1<=y2));
        in_critical++;
2:      in_critical--;
3:      y1 = 0;
  od
}

active proctype process_2() {
  do
  :: true ->
0:      y2 = y1+1;
1:      ((y1==0) || (y2<y1));
        in_critical++;
2:      in_critical--;
3:      y2 = 0;
  od
}
```

ϕ : $\Box \Diamond crit_1 \wedge \Box \Diamond crit_2$

$\mathcal{A}_\phi$



$\mathcal{A}_\mathcal{M}$



$P(\phi) > 0.95$

CONICET

UNC

UNIVERSITÄT DES SAARLANDES

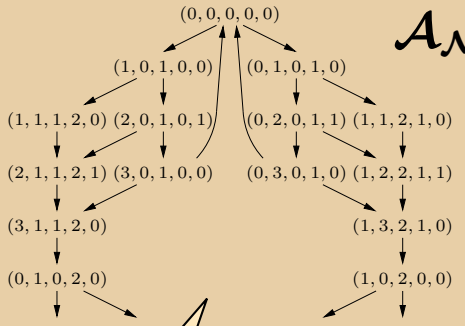
Model Checking Cuantitativo

Incluye primitivas de aleatoriedad

$\mathcal{M}$

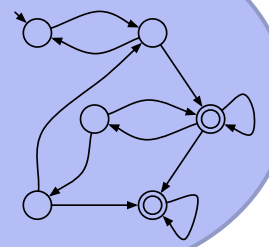
```
int y1 = 0;
int y2 = 0;
short in_critical = 0;

active proctype process_1() {
  do
  :: true ->
0:      y1 = y2+1;
1:      ((y2==0) || (y1<=y2));
        in_critical++;
2:      in_critical--;
3:      y1 = 0;
  od
}

active proctype process_2() {
  do
  :: true ->
0:      y2 = y1+1;
1:      ((y1==0) || (y2<y1));
        in_critical++;
2:      in_critical--;
3:      y2 = 0;
  od
}
```

$\mathcal{A}_\mathcal{M}$



Proceso de decisión de Markov

$\mathcal{A}_\phi$

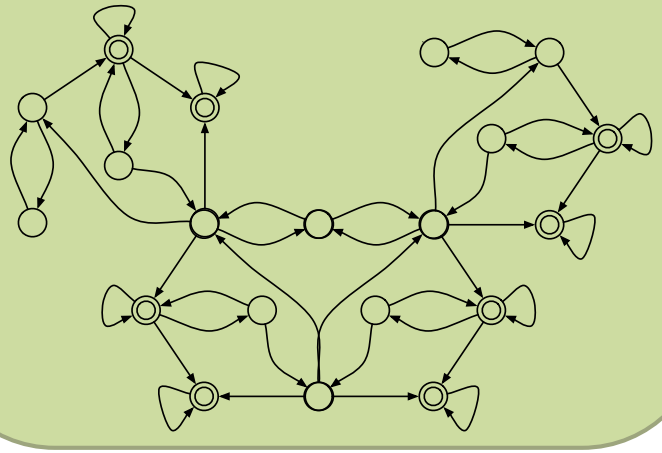


ϕ : $\Box\Diamond crit_1 \wedge \Box\Diamond crit_2$

ϕ : $\Box\Diamond crit_1 \wedge \Box\Diamond crit_2$

$\mathcal{A}_\phi$

$P(\phi) > 0.95$



Proceso de decisión de Markov

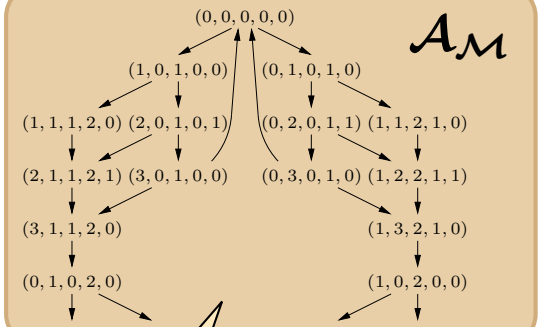
Model Checking Cuantitativo

Incluye primitivas de aleatoriedad

$\mathcal{M}$

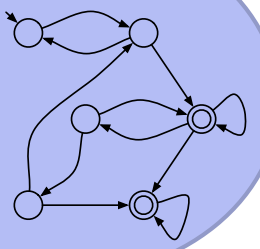
```
int y1 = 0;
int y2 = 0;
short in_critical = 0;

active proctype process_1() {
  do
  :: true ->
0:      y1 = y2+1;
1:      ((y2==0) || (y1<=y2));
        in_critical++;
2:      in_critical--;
3:      y1 = 0;
  od
}

active proctype process_2() {
  do
  :: true ->
0:      y2 = y1+1;
1:      ((y1==0) || (y2<y1));
        in_critical++;
2:      in_critical--;
3:      y2 = 0;
  od
}
```

$\mathcal{A}_{\mathcal{M}}$



Proceso de decisión de Markov

$\mathcal{A}_{\phi}$



ϕ : $\Box \Diamond crit_1 \wedge \Box \Diamond crit_2$

$\mathcal{A}_{\phi}$

¿ $\mathcal{M} \models \phi$?

Se reduce a un problema de optimización lineal

$$P(\phi) > 0.95$$

$$x_s = \max_{a \in A} \sum_{t \in S} \mathbf{P}_a(s,t) \cdot x_t \quad \text{if } s \in Pr^{>0}(B) \backslash B$$

$$x_s = 1 \quad \text{if } s \in B$$

$$x_s = 0 \quad \text{if } s \notin Pr^{>0}(B)$$

CONICET

UNC

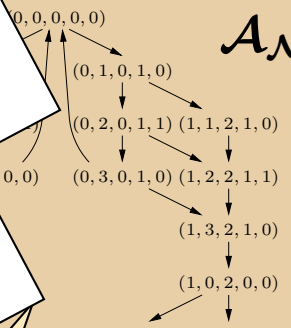
UNIVERSITÄT DES SAARLANDES

Model Checking Cuantitativo

$\mathcal{M}$

```
                                  active proctype process_2() {
                                    do
                                    :: true ->
                                0:      y2 = y1+1;
                                1:      ((y1==0) || (y2<y1));
                                        in_critical++;
                                2:      in_critical--;
                                3:      y2 = 0;
                                    od
                                  }
```

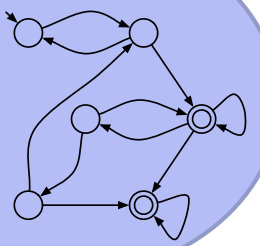
$\mathcal{A}_{\mathcal{M}}$



¿ $\mathcal{M} \models \phi$?

ϕ : $\Box \Diamond crit_1 \wedge \Box \Diamond crit_2$

$\mathcal{A}_{\phi}$



Se reduce a un problema de optimización lineal

$P(\phi) > 0.95$

$\max \sum \mathbf{P}_a(s,t) \cdot x_t$ if $s \in Pr^{>0}(B) \backslash B$

MODEST: A Compositional Modeling Formalism for Hard and Softly Timed Systems

Probabilistic Transition System Specification: Congruence and Full Abstraction of Bisimulation ⋆

SOS rule formats for convex and abstract probabilistic bisimulations*

Axiomatizing Bisimulation Equivalences and Metrics from Probabilistic SOS

A general SOS theory for the specification of probabilistic transition systems

Information and Computation

Reachability Analysis of Probabilistic Systems by Successive Refinements

Reduction and Refinement Strategies for Probabilistic Analysis

Partial Order Reduction on Concurrent Probabilistic Programs

Partial Order Reduction for Probabilistic Systems: A Re

Distributed probabilistic

Significant Diagnostic Counterexamples in Probabilistic Model Checking

Miguel E. Andrés[1,⋆], Pedro D'Argenio[2,⋆⋆], and Peter van Rossum[1]

[1] Institute for Computing and Information Sciences, The Netherlands
{mandres,petervr}@cs.ru.nl
[2] Universidad Nacional de Córdoba, CONICET, Argentina
dargenio@famaf.unc.edu.ar

Fallas

CONICET

UNC

UNIVERSITÄT DES SAARLANDES

Un sistema es resiliente si …

… tiene la habilidad de proveer y mantener un nivel de servicio aceptable aún bajo la presencia de fallas y otros inconvenientes que puedan surgir y presentar un desafío al funcionamiento normal del sistema.

¿Cómo enfrentar las fallas?

CONICET

UNC

UNIVERSITÄT DES SAARLANDES

Cómo enfrentar las fallas

1. Failover: Varias componentes idénticas de respaldo. Cuando la componente principal falla el sistema lo detecta y cambia a una de las de respaldo.

2. Votación: Varias componentes idénticas activas. La información correcta se decide por votación.

3. Detección y corrección de errores: Redundancia de información en los datos.

4. Reconocimientos (Acks) y timeouts: Reconocimiento de entrega y repetición de la información sospechada perdida.

Eventos

Los eventos pueden cuantificarse probabilísticamente

Ejemplos:

- Probabilidad de pérdida de un mensaje
- Tiempo esperado de vida de una fuente de alimentación
- Tiempo esperado de reparación del disco rígido
- Tiempo esperado de transmisión tierra-satélite
- Probabilidad de alteración de un bit bajo radiación
- Tiempo esperado de refrescado de memoria

(Algunas) Técnicas de análisis

- Model checking cuantitativo

  Ya lo vimos

- Simulación por eventos discretos

  En particular nos interesa la simulación de eventos raros

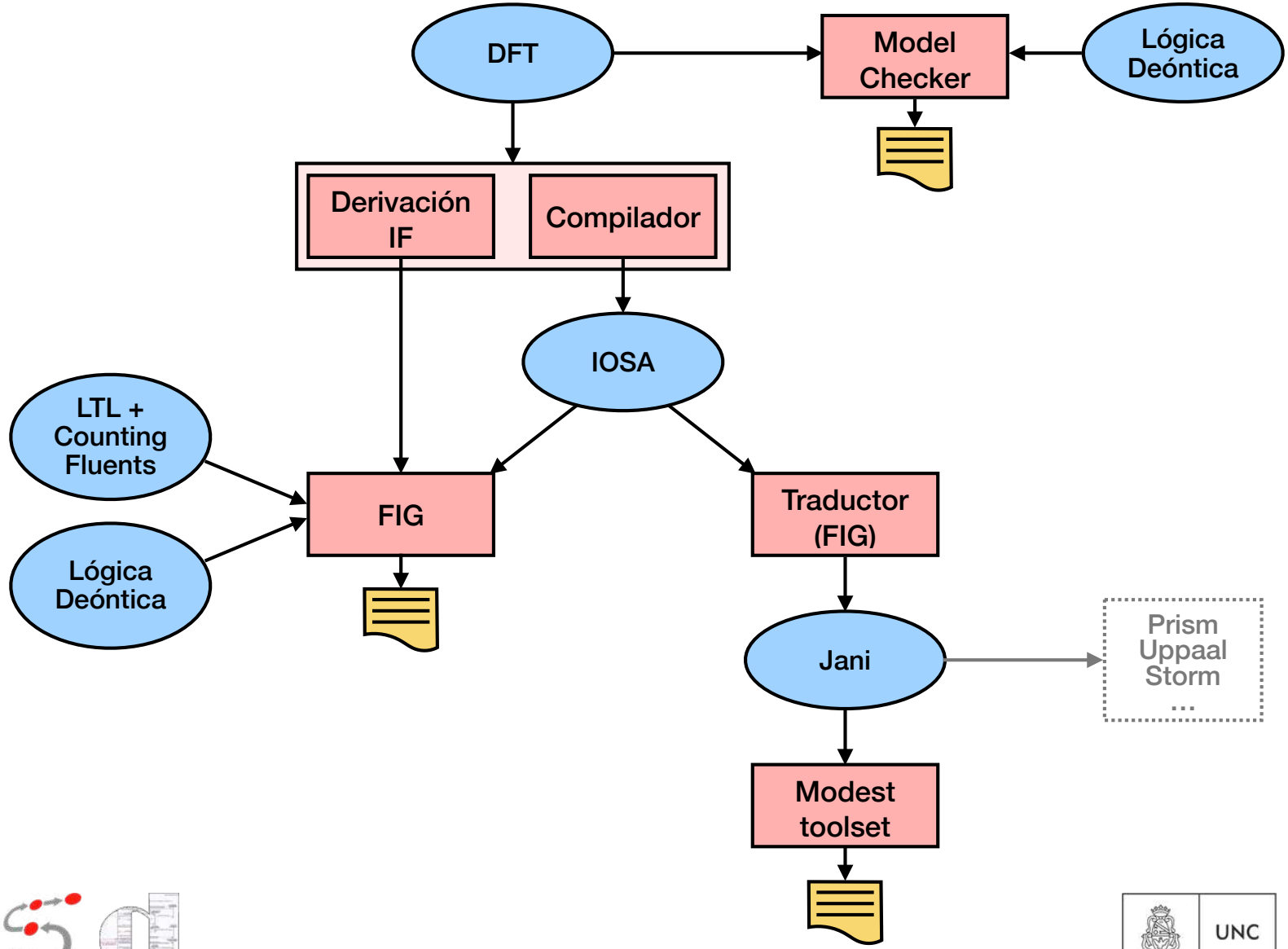
  es decir, de muy baja probabilidad

- Model checking estadístico

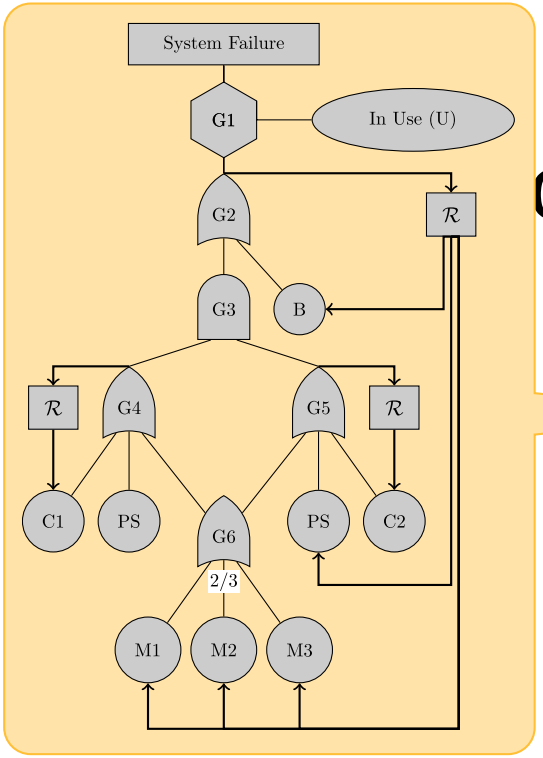
  Es una variante específica de la simulación

  + no-determinismo

Proyectos RAFTSys y ARES



oyectos RAFTSys y ARES



DFT

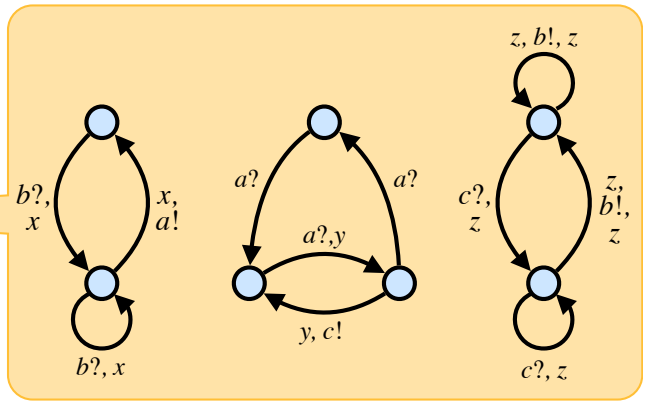
Model Checker

Lógica Deóntica

Derivación IF

Compilador

IOSA



LTL + Counting Fluents

Lógica Deóntica

FIG

Traductor (FIG)

Jani

Prism
Uppaal
Storm
...

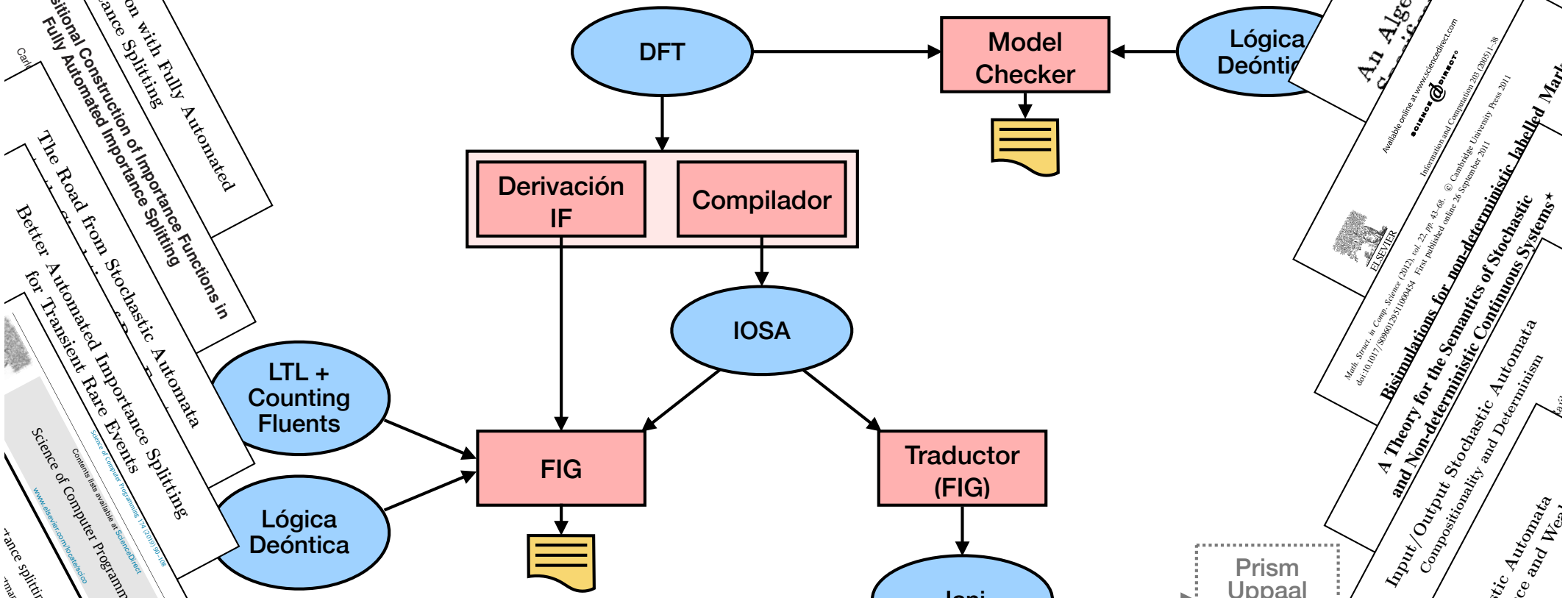
Modest toolset

CONICET

UNC

UNIVERSITÄT DES SAARLANDES

Proyectos RA RES



Proyectos RAFTSys y ARES

dargenio@famaf.unc.edu.ar

Redes de Satélites

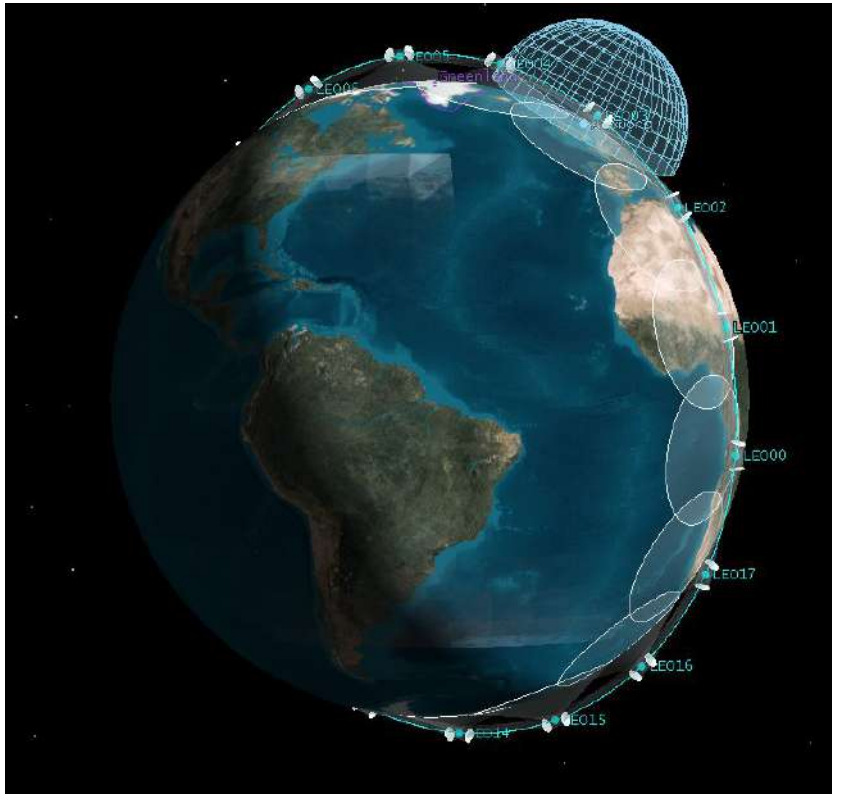
GomSpace (DK)

Redes de Satélites

GomSpace (DK)

Redes de Satélites

GomSpace (DK)

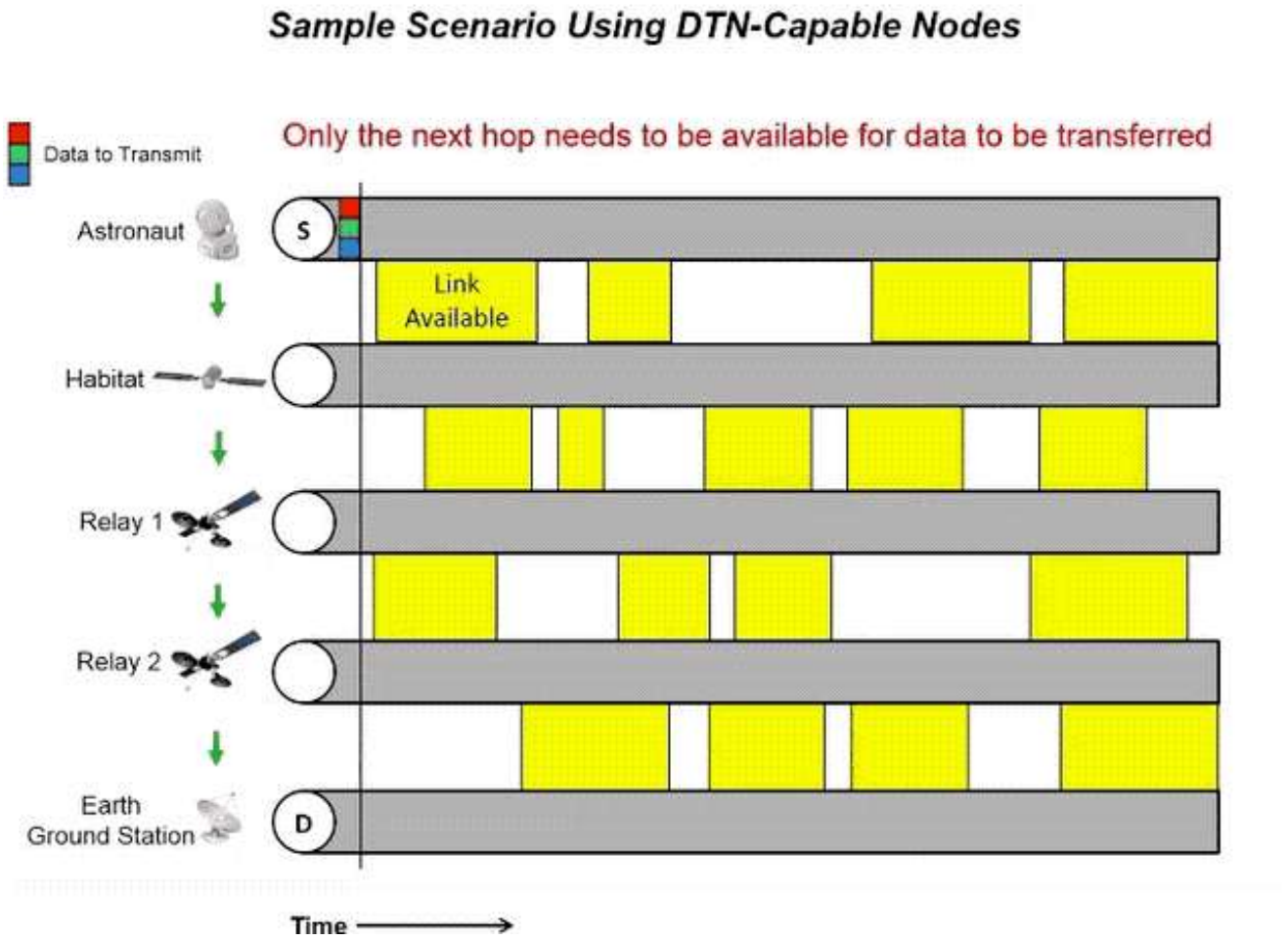


CONICET

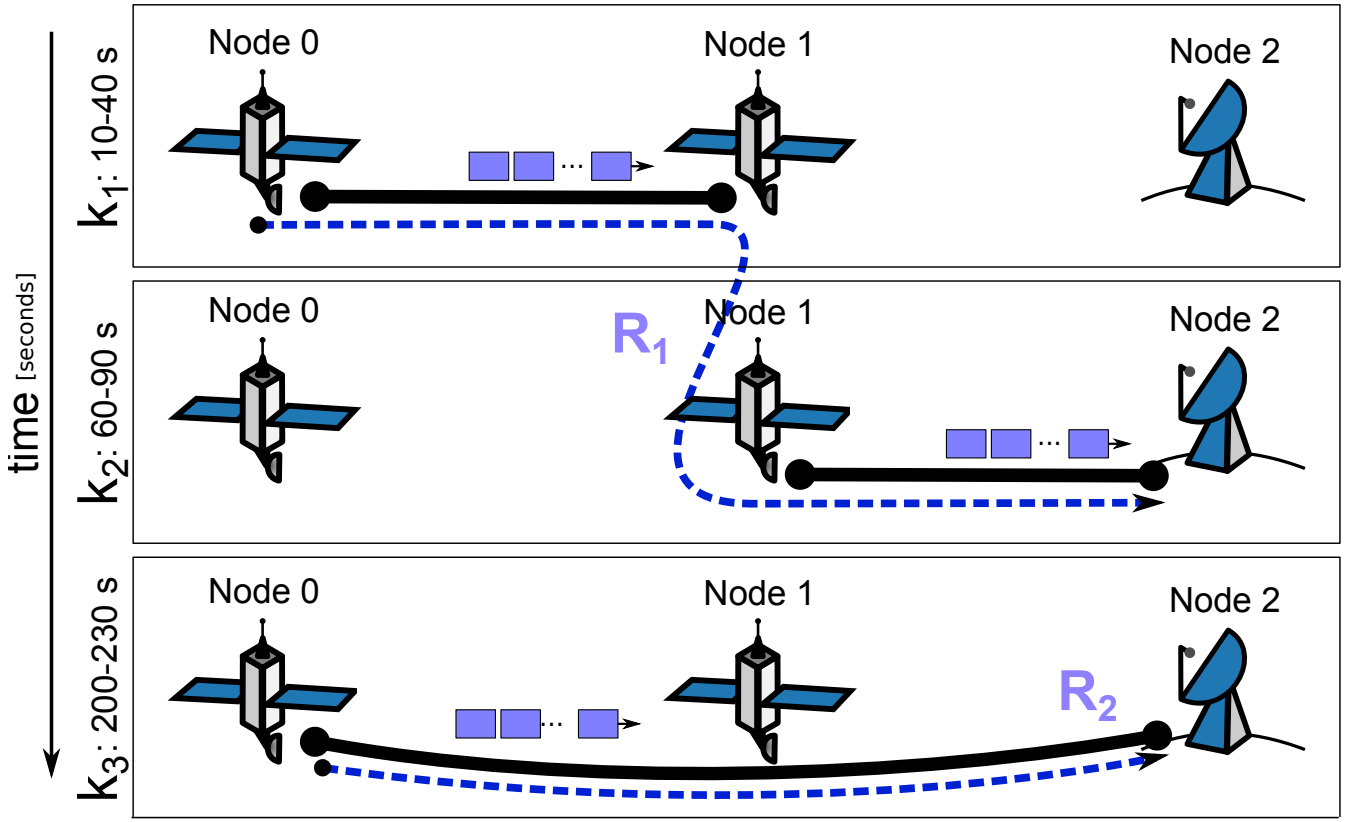
UNC

UNIVERSITÄT DES SAARLANDES

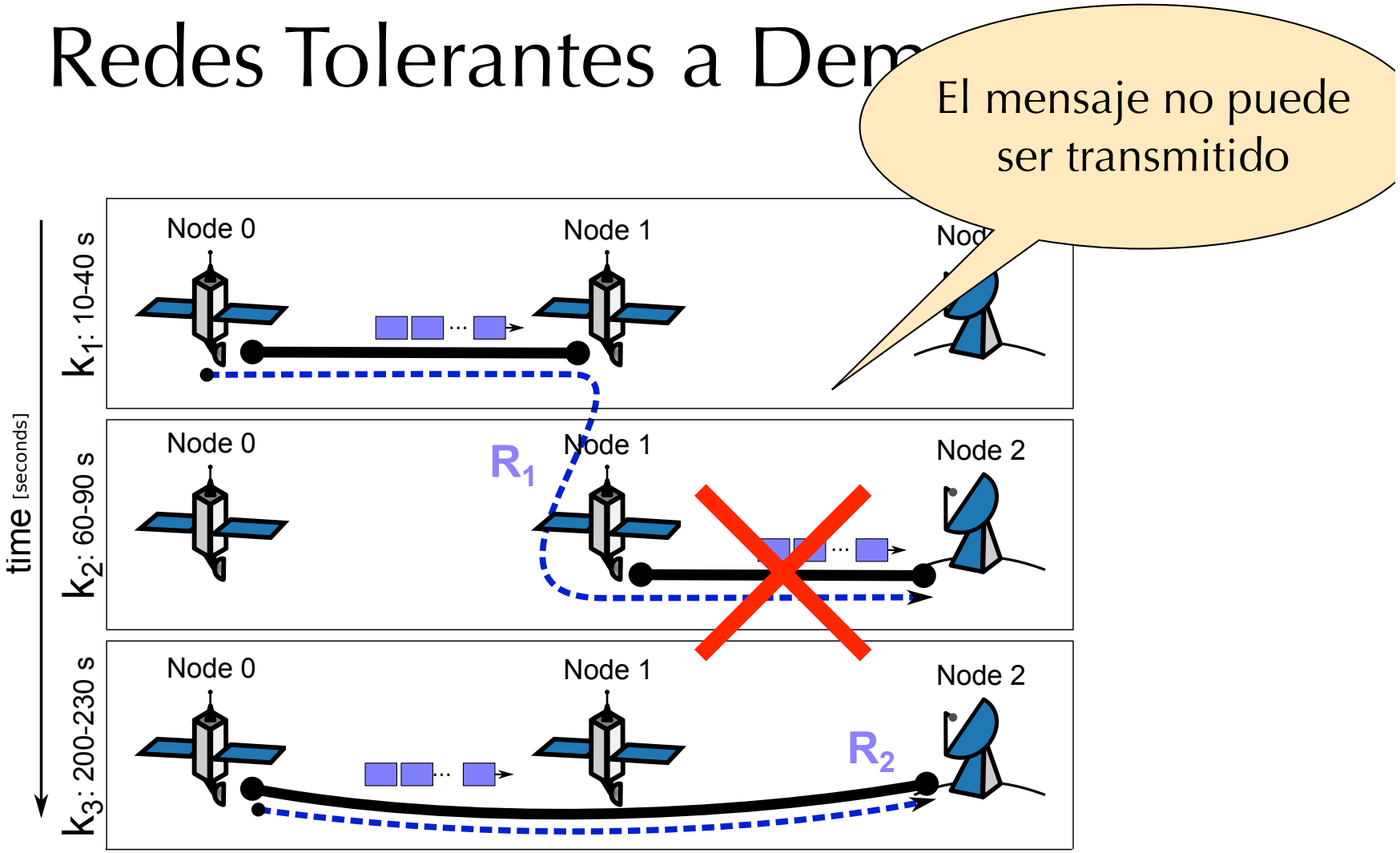
Redes Tolerantes a Demora



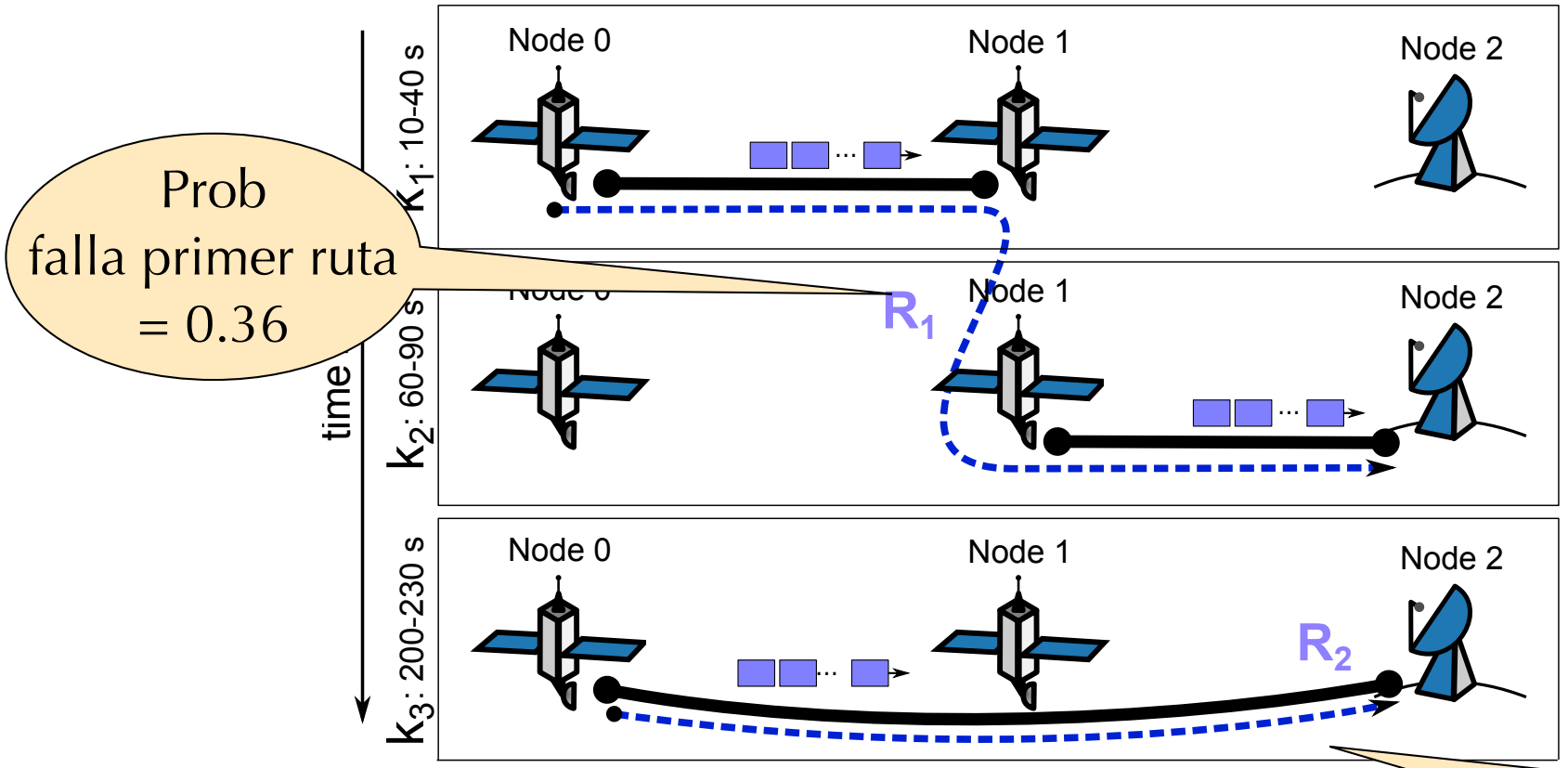
Redes Tolerantes a Demora



Redes Tolerantes a Dem

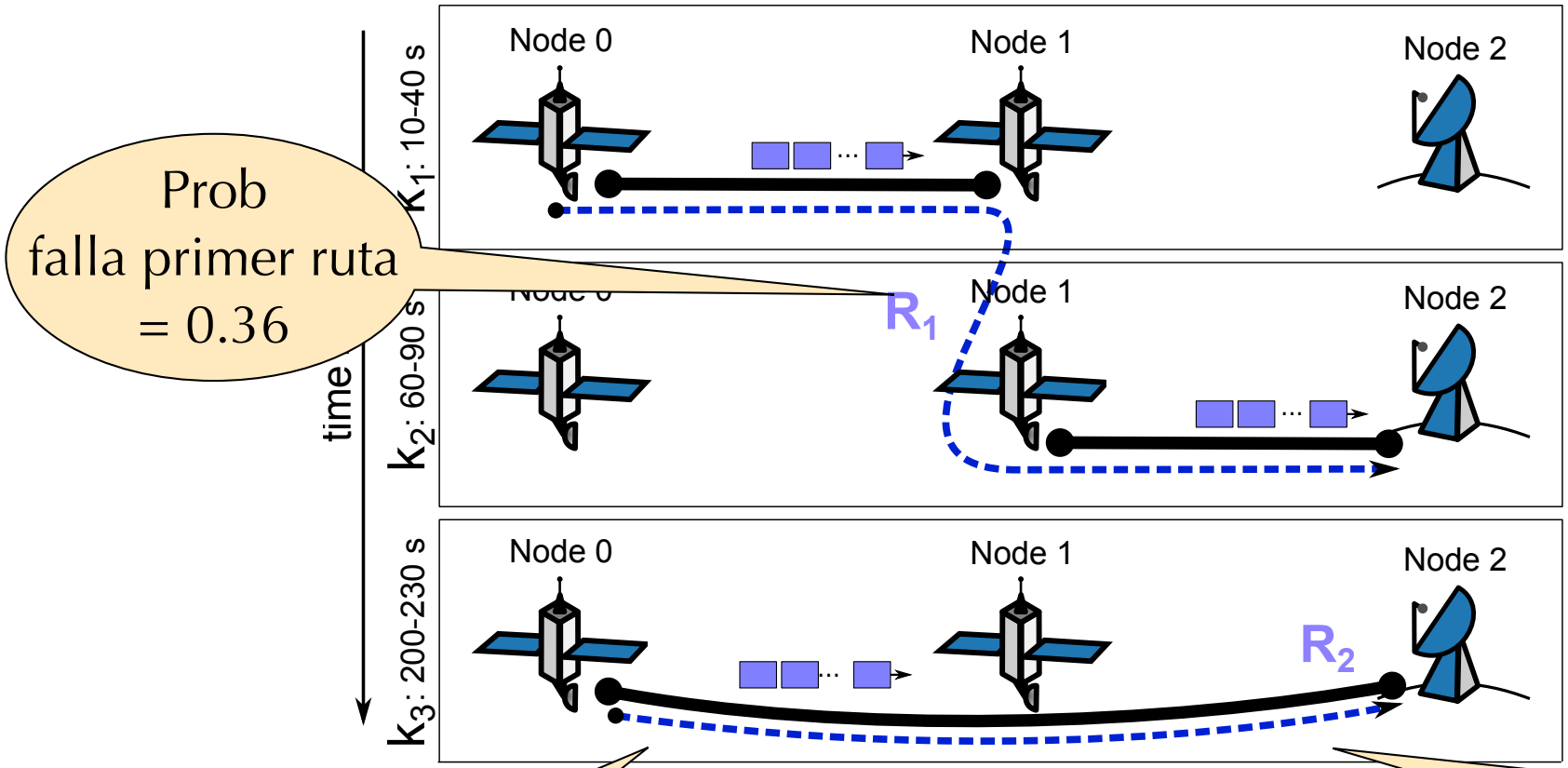


Redes Tolerantes a Demora



Probabilidad de falla de un link = 0.2

Redes Tolerantes a Demora



Prob falla primer ruta = 0.36

Síntesis de ruteo usando Model Checking Cuantitativo

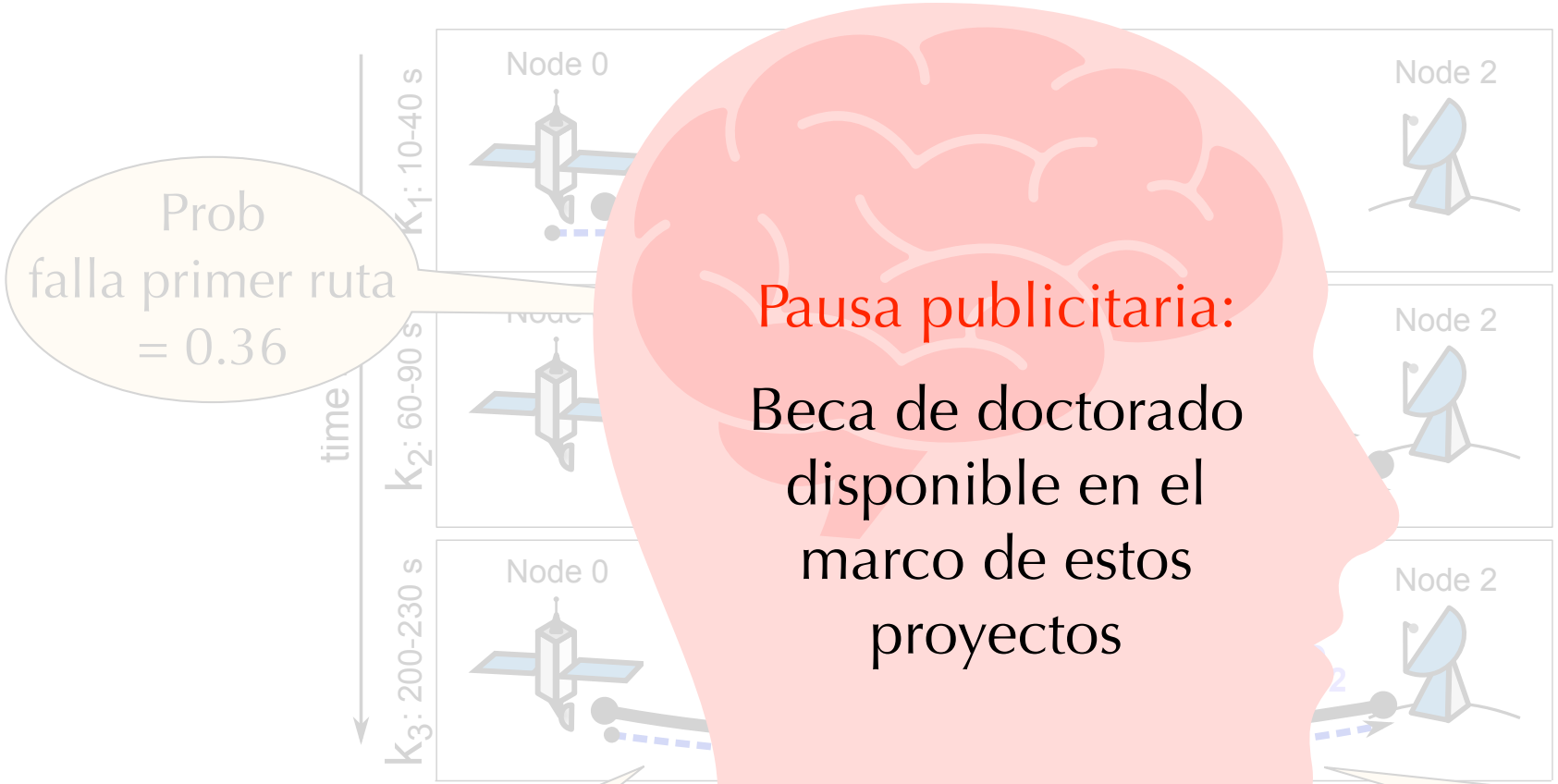
bilidad de falla de un link = 0.2

Prob falla segunda ruta

A Markov Decision Process for Routing in Space DTNs with Uncertain Contact Plans

Fernando D. Raverta*†, Ramiro Demasi*‡, Pablo G. Madoery*†, Juan A. Fraire*‡§,
Jorge M. Finochietto*†, Pedro R. D'Argenio*‡§
Instituto de Investigaciones Científicas y Técnicas (CONICET), Córdoba, Argentina
Facultad de Matemática, Física y Naturales (FCEFyN), UNC. Córdoba, Argentina
Facultad de Matemática, Física y Computación (FAMAF), UNC, Córdoba, Argentina
Saarland University, Saarbrücken, Germany

Proyectos RAFTSys y ARES



Prob falla primer ruta = 0.36

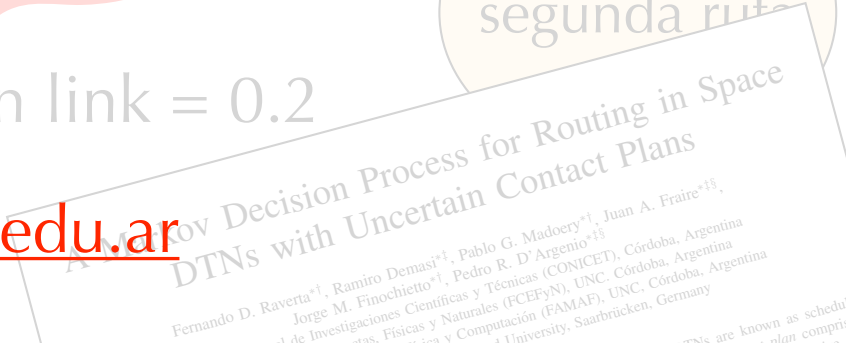
Pausa publicitaria:

Beca de doctorado disponible en el marco de estos proyectos

Síntesis de ruteo usando Model Checking Cuantitativo

Prob falla segunda ruta

un link = 0.2



dargenio@famaf.unc.edu.ar

Fallutadas abusivas

Estrategias de
"lock in"

Fallutadas famosas

Fallutadas famosas

UNC

UNIVERSITÄT DES SAARLANDES

Fallutadas famosas

UNC

UNIVERSITÄT DES SAARLANDES

Fallutadas famosas

Lifestyle › Cars › News

Diesel emissions scandal: Fiat under investigation

Germany orders Porsche recall over diesel emissions cheating

May 18, 2018

Business | Companies | Markets | Finance | Regulation

VW scandal: Carmaker was warned by Bosch about test-rigging software in 2007

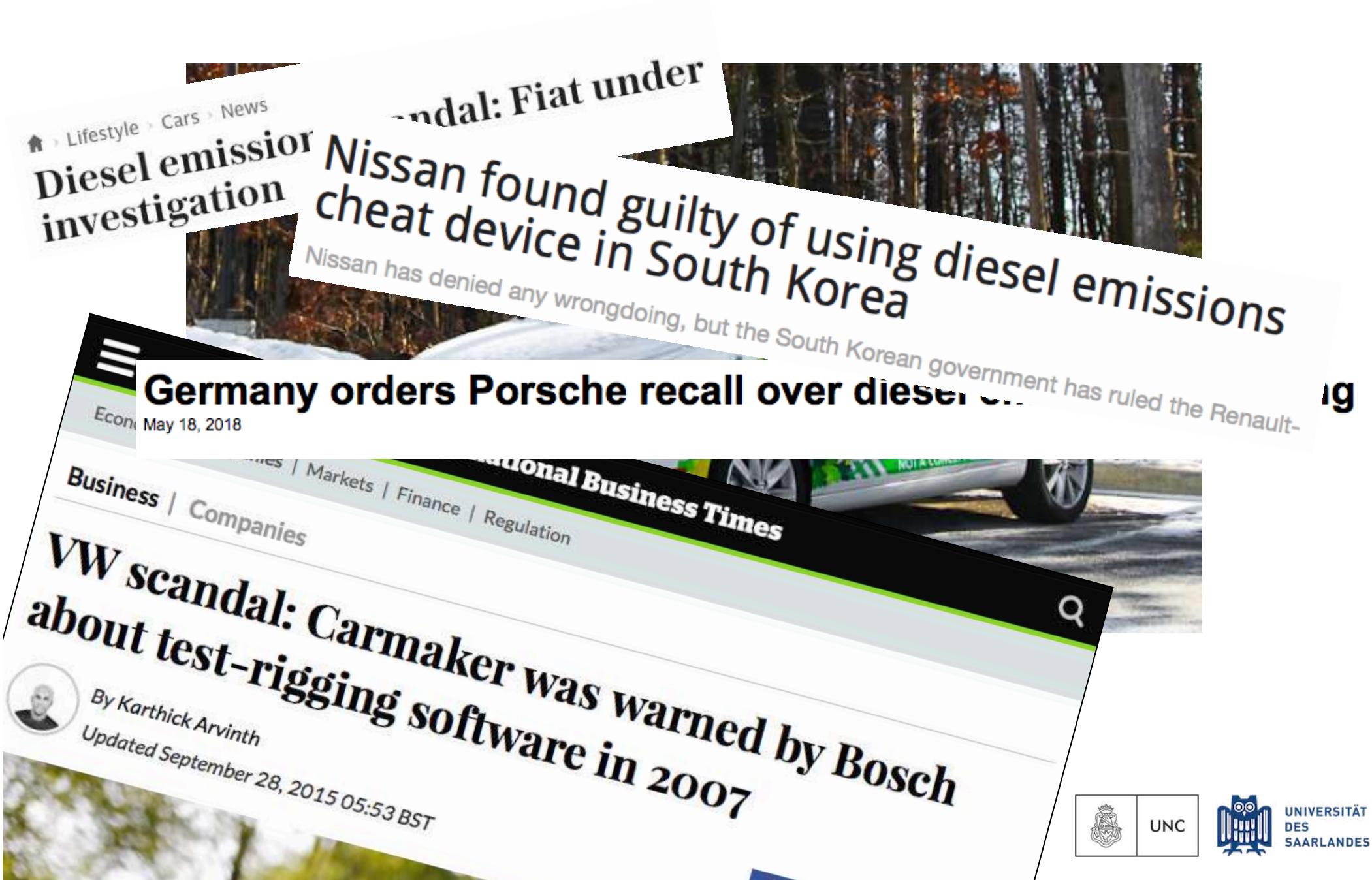
By Karthick Arvinth

Updated September 28, 2015 05:53 BST

UNC

UNIVERSITÄT DES SAARLANDES

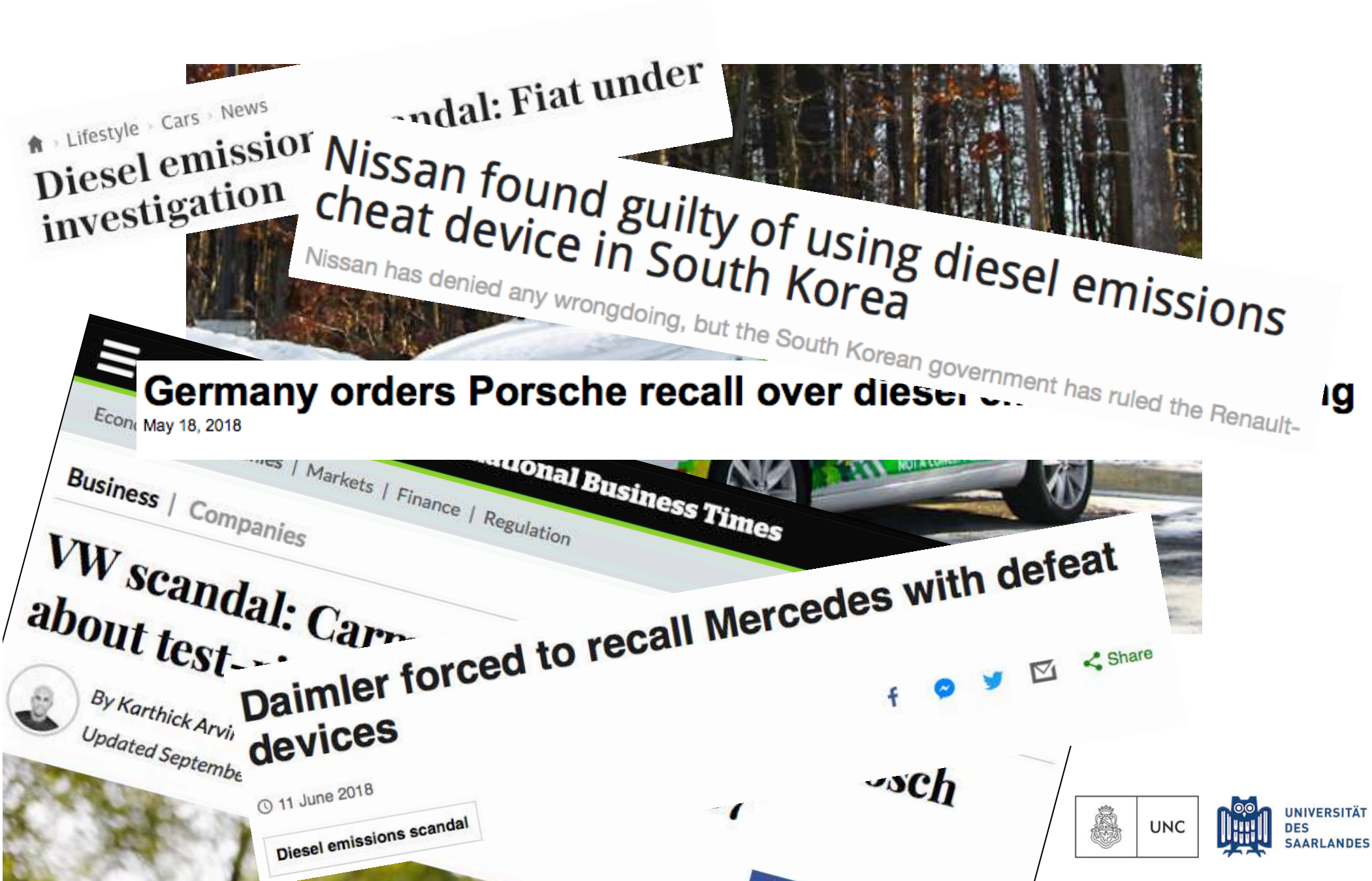
Fallutadas famosas



UNC

UNIVERSITÄT DES SAARLANDES

Fallutadas famosas



UNC

UNIVERSITÄT DES SAARLANDES

Fallutada

France

Peugeot suspected of fraud in diesel scandal

PSA Peugeot Citroën | French economy | auto industry

Share 1 Tweet Share Share

Lifestyle › Cars › News

Diesel emissior investigation

Nissan found guilty of using diesel emissi cheat device in South Korea

Nissan has denied any wrongdoing, but the South Korean government has ruled the Renault-

Germany orders Porsche recall over diesel

May 18, 2018

Business | Companies | Markets | Finance | Regulation

National Business Times

VW scandal: Carm about test-

By Karthick Arvi

Updated Septembe

Daimler forced to recall Mercedes with defeat devices

Share

11 June 2018

Diesel emissions scandal

osch

UNC

UNIVERSITÄT DES SAARLANDES

Fallutada


France
Peugeot suspected of fraud in diesel scandal
PSA Peugeot Citroën | French economy | auto industry
Share 1
Tweet
Share
Share
Lifestyle › Cars › News
Diesel emissio
investigation
Nissan found guilty of using diesel emissi
cheat device in South Korea
Nissan has denied any wrongdoing, but the South Korean government has ruled the Renault-
Germany orders Porsche recall over diesel
May 18, 2018
Business | Companies
Markets | Finance | Regulation
National Business Times
VW scandal: Carm
about test-
to recall Mercedes with defeat
Share
By Karthick Arvi
Updated Septembe
Renault 'cheated on 25 years of pollution tests'
11 June 2018
Diesel emissions scandal

Fallutada

France

Peugeot suspected of fraud in diesel scandal

PSA Peugeot Citroën | French economy | auto industry

Share 1 Tweet Share Share

Lifestyle › Cars › News

Diesel emissior investigation

Nissan found guilty of using diesel emissi cheat device in South Korea

Nissan has denied any wrongdoing, but the South Korean government has rule

Germany orders Porsche recall over diesel

May 18, 2018

Business | Companies

VW scandal: Carm about test-

By Karthick Arvi

Updated Septembe

Citroën may have breached emissions rules: report

A model tested by the European Commission recorded pollution levels more t

d to recall Mercedes with defeat

Share

Renault 'cheated on 25 years of pollution tests'

11 June 2018

Diesel emissions scandal

Fallutada


France
Peugeot suspected of fraud in diesel scandal
PSA Peugeot Citroën | French economy | auto industry
Share 1
Tweet
Share
Lifestyle › Cars › News
Diesel emissior
investigation
Nissan found gu
cheat device in S
Nissan has denied any wrongdoing, but the South Korean government has
GM Accused of Cheating on Diesel Emissions
Germany orders Porsche recall over diesel
May 18, 2018
Business | Companies
VW scandal: Carm
about test-
By Karthick Arvi
Updated Septembe
Citroën may have breached emissions rules: report
A model tested by the European Commission recorded pollution levels more t
to recall Mercedes with defeat
Share
Renault 'cheated on 25 years of pollution tests'
11 June 2018
Diesel emissions scandal

Fallutadas imperdonables

https://www.mintpressnews.com/214505-2/214505/

Software doping

- Es un problema ético y hasta legal.

- Un software está "dopado" si…

  … el fabricante incluyó una funcionalidad oculta de manera tal que el comportamiento resultante favorezca intencionalmente a una parte previamente designada, en contra de los intereses de la sociedad o el licenciatario del software

Software doping

- Es un problema ético y hasta legal.

Pero …
propusimos una solución técnica (formal)

- Un software está "dopado" si…

… el fabricante incluyó una funcionalidad oculta de manera tal que el comportamiento resultante favorezca intencionalmente a una parte previamente designada, en contra de los intereses de la sociedad o el licenciatario del software

No es posible de formalizar

CONICET

UNC

UNIVERSITÄT DES SAARLANDES

Software doping

definición formal

- Memoria: $\mu : \mathit{Variables} \to \mathit{Valores}$
- Un programa es un transformador de memoria: $(S, \mu) \Downarrow \mu'$
- Variables:

  Entrada de interés: $i \in \mathit{Variables}$ Salida de interés: $o \in \mathit{Variables}$

- Software doping

S *no está dopado* si para todas μ_1, μ_2, μ'_1 y μ'_2,

$$\left.\begin{array}{l} \mu_1(i) \approx \mu_2(i) \\ (S, \mu_1) \Downarrow \mu'_1 \\ (S, \mu_2) \Downarrow \mu'_2 \end{array}\right\} \Rightarrow \quad \mu'_1(o) \approx \mu'_2(o)$$

"se parece"

CONICET UNC UNIVERSITÄT DES SAARLANDES

Software doping

definición formal

- Memoria: $\mu : \mathit{Variables} \to \mathit{Valores}$
- Un programa es un transformador de memoria: $(S, \mu) \Downarrow \mu'$
- Variables:

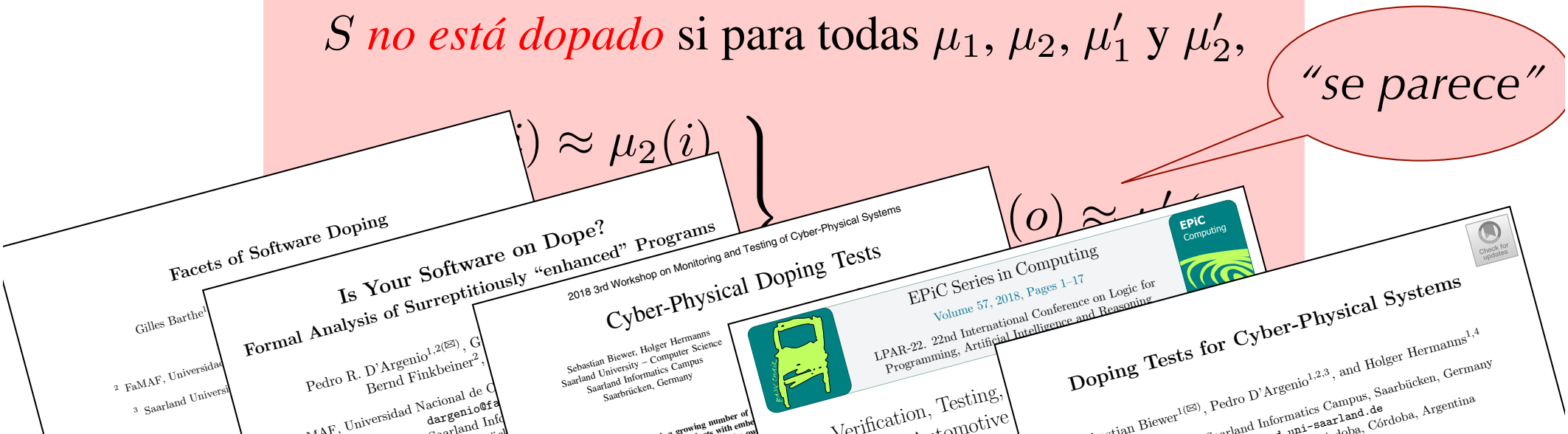
  Entrada de interés: $i \in \mathit{Variables}$ Salida de interés: $o \in \mathit{Variables}$

- Software doping

S *no está dopado* si para todas μ_1, μ_2, μ'_1 y μ'_2,

$$\left.\begin{array}{l} \\ \\ \end{array}\right\} \quad (o) \approx$$

"se parece"



¿Qué conclusión sacan ustedes?

Las que saco yo:

Las técnicas formales (matemáticas) son cruciales para todo esto

- No está bueno echarse moco
  - ➡ hacer lo posible por evitarlos y eliminarlos
- Las fallas inevitablemente ocurren
  - ➡ tratar efectivamente con ellas y de manera eficiente
- Las fallutadas son una mala costumbre de la disciplina
  - ➡ No sólo contrarrestarlas ética y legalmente sino también técnicamente

Epílogo perturbador

Preferencias de Materias Optativas (estudiantes)

Departamento de Computación FCEyN, UBA

Introducción al Procesamiento del Lenguaje Natural	29
Programación de Sistemas Operativos	29
Aprendizaje Automático	27
Ciencia de Datos	25
Aprendizaje Profundo / Redes Neuronales Profundas	20
Programación Concurrente	20
Algoritmos y Estructuras de Datos Avanzadas / Problemas de Grafos y Tratabilidad Computacional	19
Seguridad de la Información	19
Arquitectura de Aplicaciones Web	17
Programación Orientada a Objetos/Diseño Avanzado de Objetos	17
Computación Móvil	13
Investigación Operativa	12
Generación Automática de Casos de Test	10
Problemas, Algoritmos y Programación	10
Redes Neuronales	9
Redes, Sociedad y Economía	9
Inferencia Bayesiana	8
Simulación de Eventos Discretos	8
Computación, Ciencia y Sociedad en la Argentina	7
Computación Gráfica	7
Introducción a la Robótica Móvil	7
Metaheurísticas	7

Preferencias de Materias Optativas (estudiantes)

Departamento de Computación FCEyN, UBA

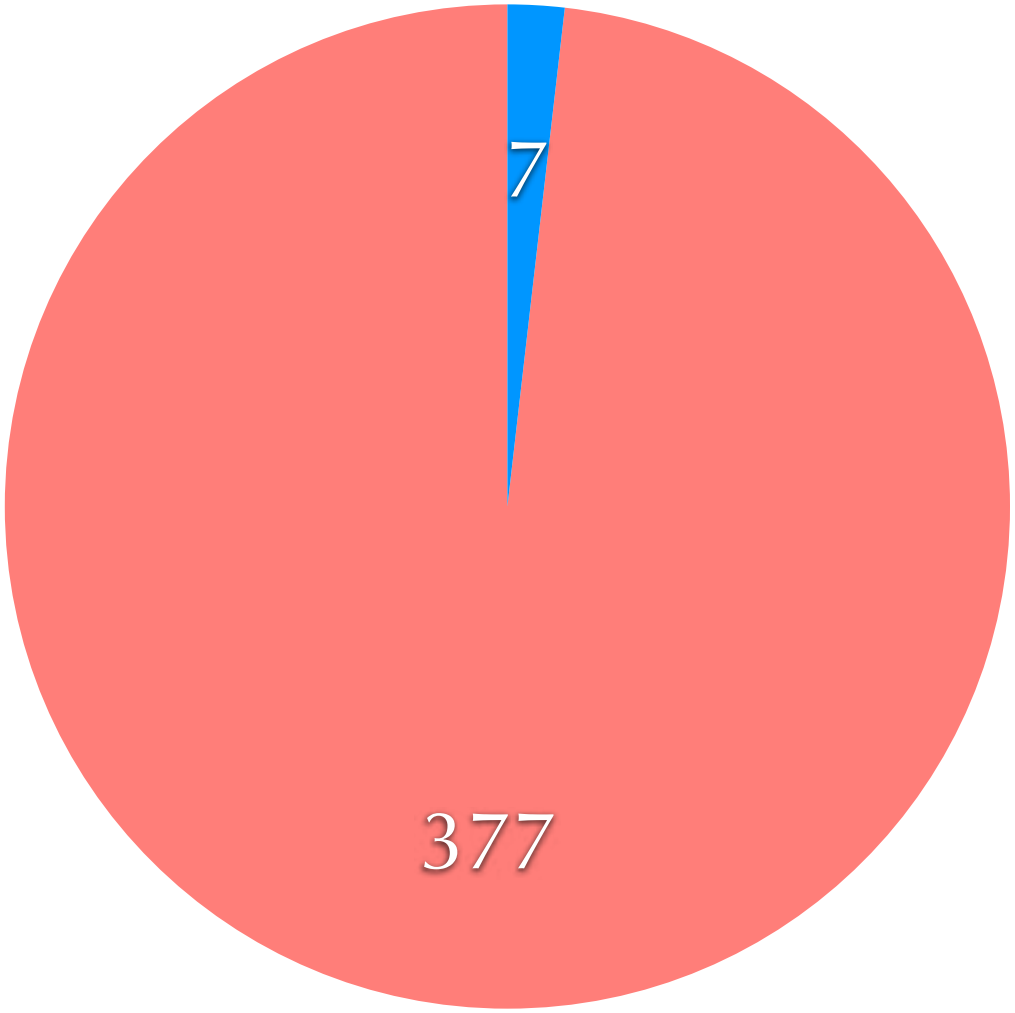
Simulación de Eventos Discretos	8
Computación, Ciencia y Sociedad en la Argentina	7
Computación Gráfica	7
Introducción a la Robótica Móvil	7
Metaheurísticas	7
Introducción al Procesamiento Digital de Imágenes	6
Reconocimiento de Patrones	6
Reescritura (Cálculo Lambda)	6
Teoría de la computabilidad	6
Arquitectura y Comunicación de Datos	4
Visión en Robótica	4
Introducción al Análisis Formal de Normas Legales	3
Seminario sobre Algoritmos de Análisis de Secuencias Biológicas	3
Sistemas Complejos	3
Validación y Verificación de Programas	3
Visión por Computadora	3
Seminario Avanzado de Programación Lineal Entera -	2
Análisis y Síntesis Automática de Programas	1
Fundamentos de Especificación de Software	1
Reglas de Asociación y Patrones Secuenciales -	1
Seminario Avanzado de Análisis de Programas	1
Seminario Avanzado sobre Modelos y Algoritmos para el Análisis de Sistemas	1
Integración de Bases de Conocimiento	1

CONICET

SAARLANDES

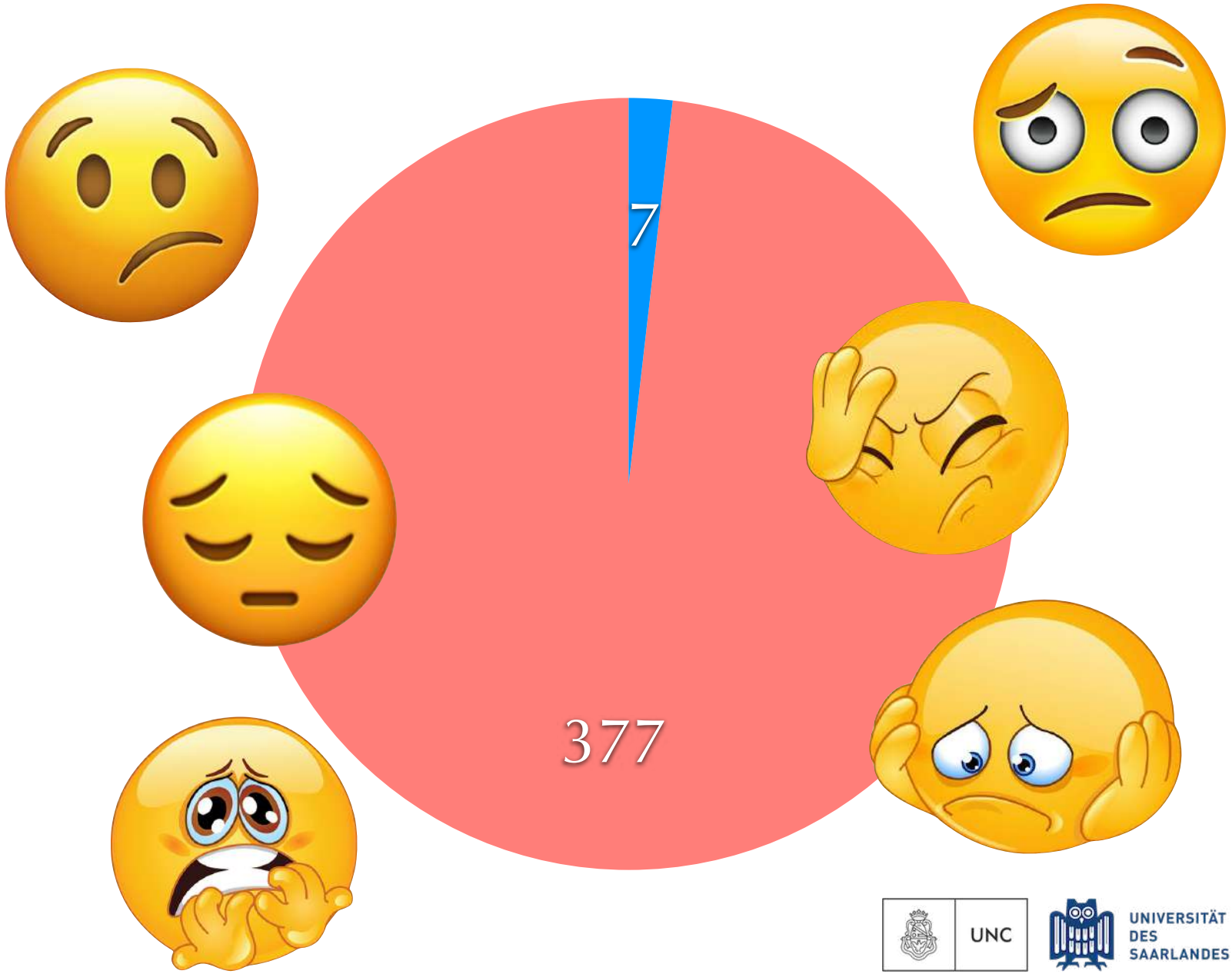
Preferencias de Materias Optativas
(estudiantes)
Departamento de Computación
FCEyN, UBA

Sólo el 1.8% pondera la importancia de la corrección y la confiabilidad



Preferencias de Materias Optativas
(estudiantes)
Departamento de Computación
FCEyN, UBA

Sólo el 1.8% pondera la importancia de la corrección y la confiabilidad



CONICET

UNC

UNIVERSITÄT DES SAARLANDES

Moco, Falla y Fallutada:
Los supervillanos del universo SC*

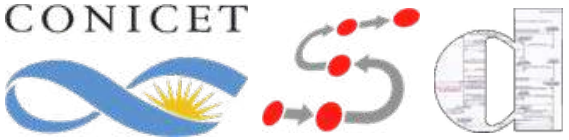
(* Sistemas Confiables)

Pedro R. D'Argenio

Grupo de Sistemas Confiables

Universidad Nacional de Córdoba – CONICET (AR)

Saarland University (DE)



Mes de la Ciencia 2019 - FAMAF