Università degli studi di Cagliari
Facoltà di Ingegneria
Dipartimento di Ingegneria Elettrica ed Elettronica
Corso di Laurea Magistrale in Ingegneria Elettronica

Université de Lorraine
Institut National Polytechnique de Lorraine
École nationale supérieure d'électricité et de mécanique
Ingenérie des Systèmes Automatisés

Deterministic and probabilistic dependability assessments of a critical system

Candidato: Bruno Pinna

Relatore: Prof. Alessandro Giua

Controrelatore: Prof.ssa Carla Seatzu

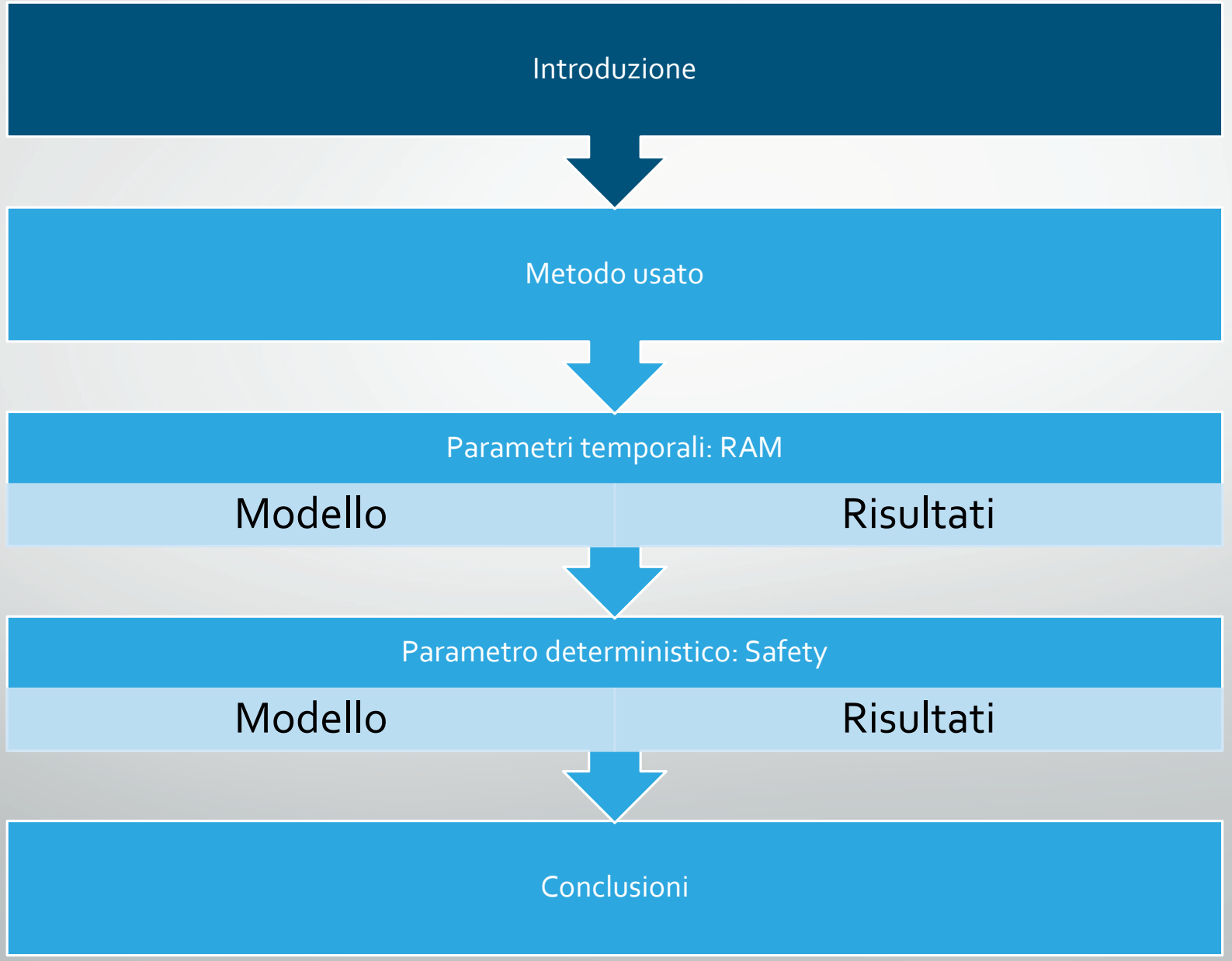
Supervisori esteri:

Ph.D. Génia Babykina

Prof. Nicolae Brînzei

Prof. Jean-François Petin

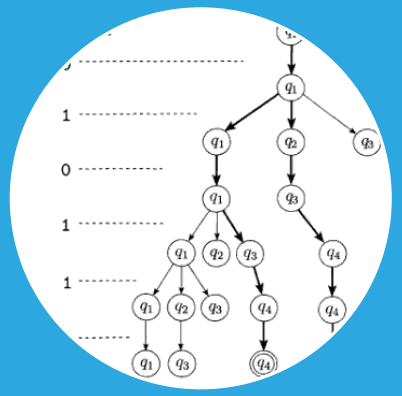
Outline


Introduzione
Metodo usato
Parametri temporali: RAM
Modello
Risultati
Parametro deterministico: Safety
Modello
Risultati
Conclusioni

Introduzione

Fidatezza

RAMS



Modello matematico

Automi

Model checking

LTL

Introduzione

Il caso studiato

Progetto APPRODYN

APProches de la fiabilité DYNamique pour modéliser des systèmes critiques

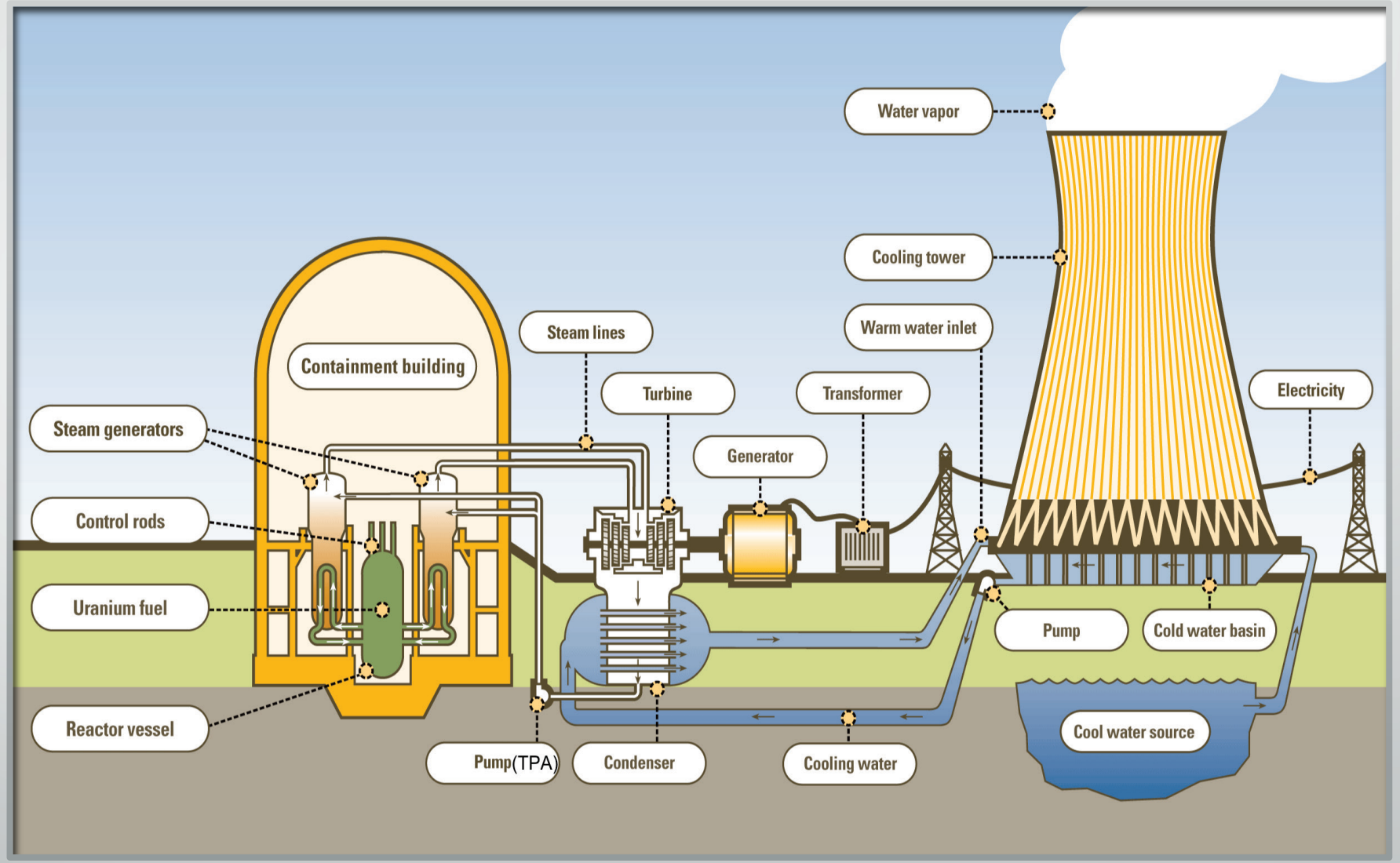


Fig.1 : Schema di una centrale nucleare ad acqua pressurizzata (PWR)

Introduzione

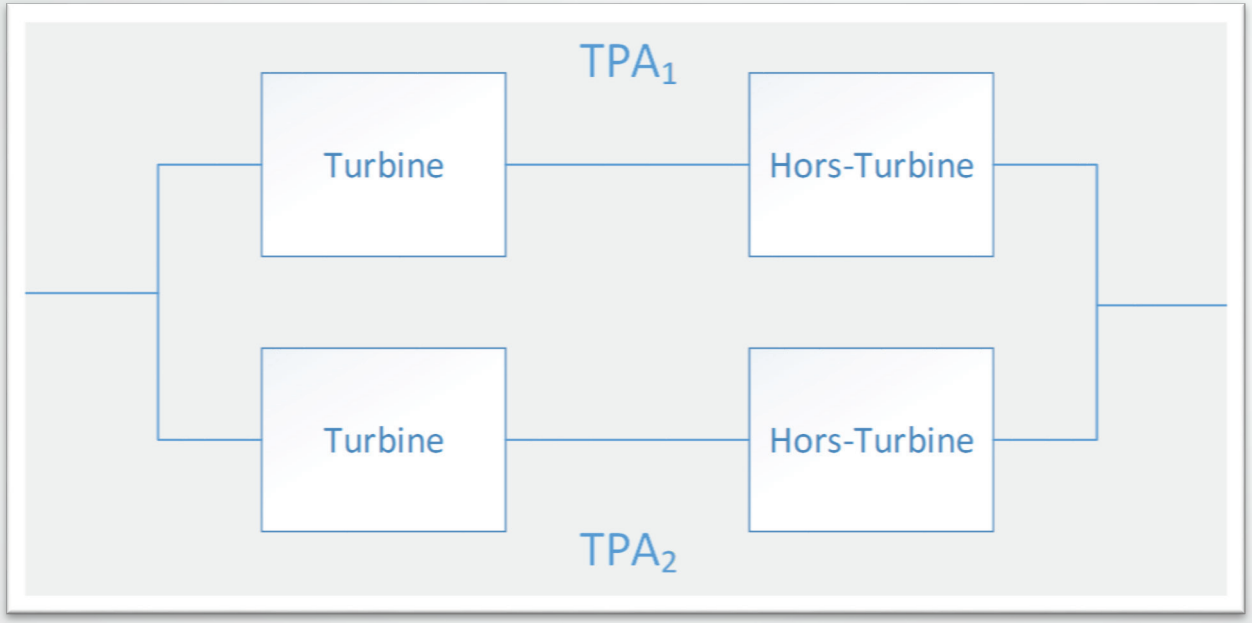


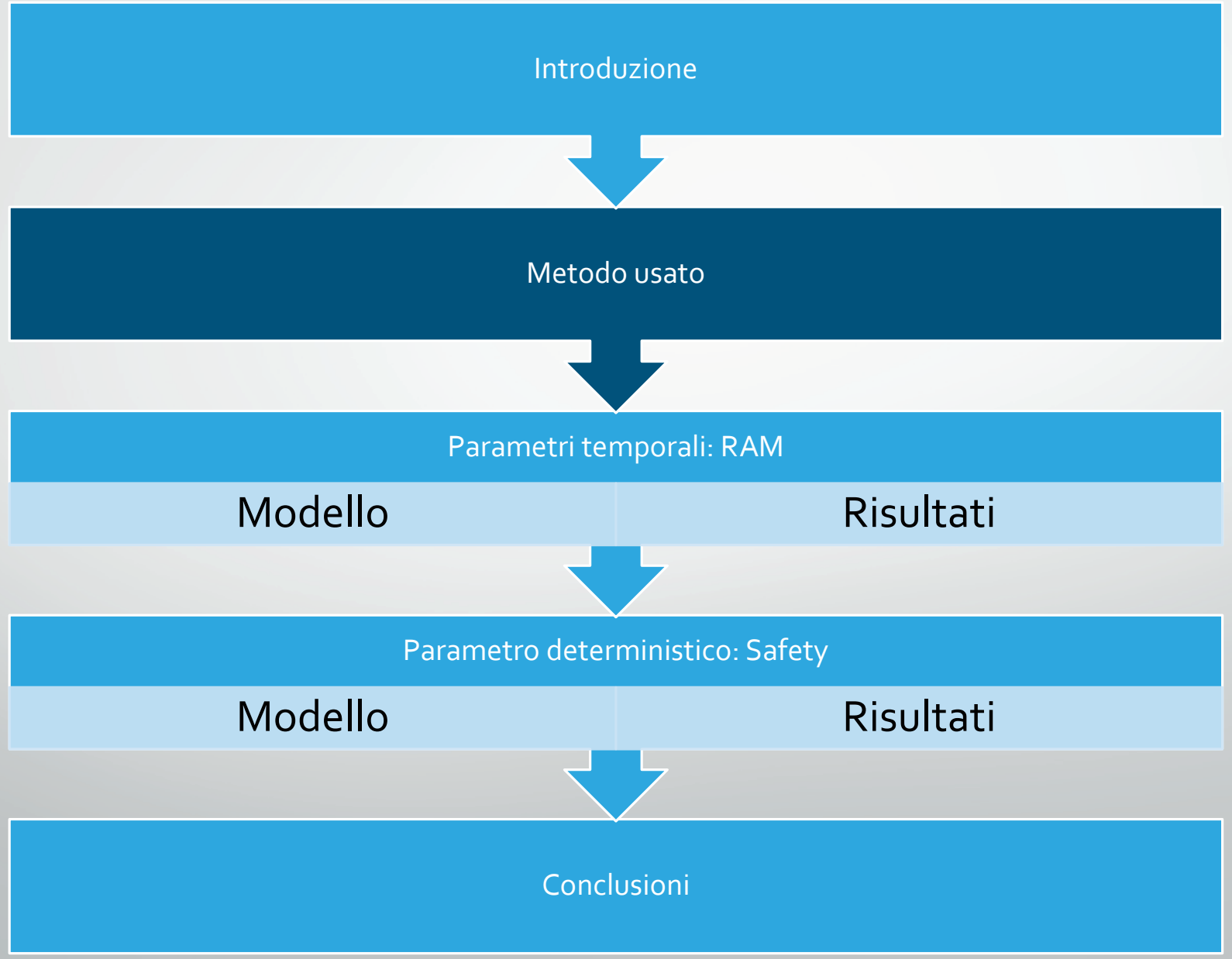
Fig.2: Diagramma di affidabilità del sistema

	λ_T [h]$^{-1}$	λ_{HT} [h]$^{-1}$	μ_T [h]$^{-1}$	μ_{HT} [h]$^{-1}$
TPA1	$1.47 \cdot 10^{-4}$	$1.46 \cdot 10^{-4}$	$5 \cdot 10^{-5}$	$4{,}17 \cdot 10^{-2}$
TPA2	$4.42 \cdot 10^{-4}$	$1.47 \cdot 10^{-7}$	$4{,}17 \cdot 10^{-3}$	$6.94 \cdot 10^{-3}$

λ: Tasso di guasto
μ: Tasso di riparazione

Tab.1: Parametri del sistema

Outline


Introduzione
Metodo usato
Parametri temporali: RAM
Modello
Risultati
Parametro deterministico: Safety
Modello
Risultati
Conclusioni

Metodo usato

OBIETTIVI

Probabilistici

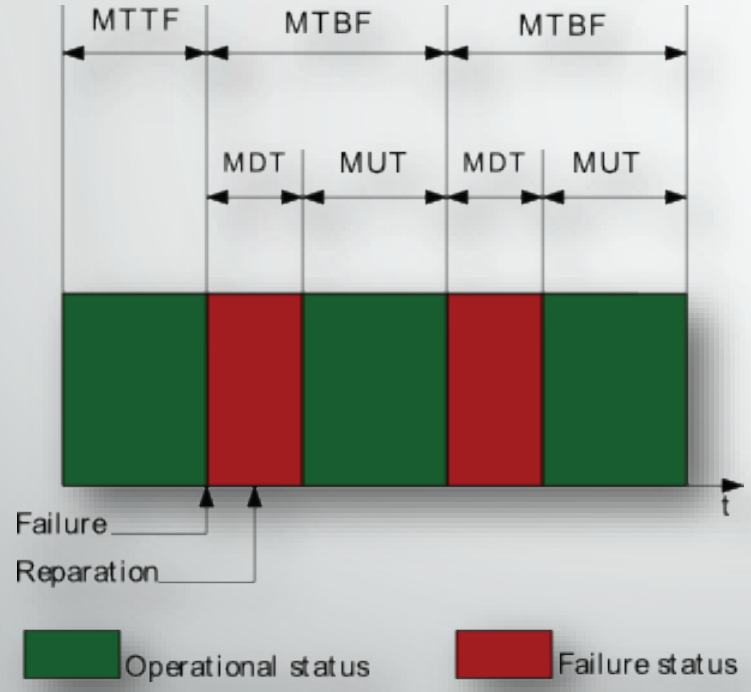


Fig.3 : Parametri associati alla fidatezza (RAM)

Deterministici

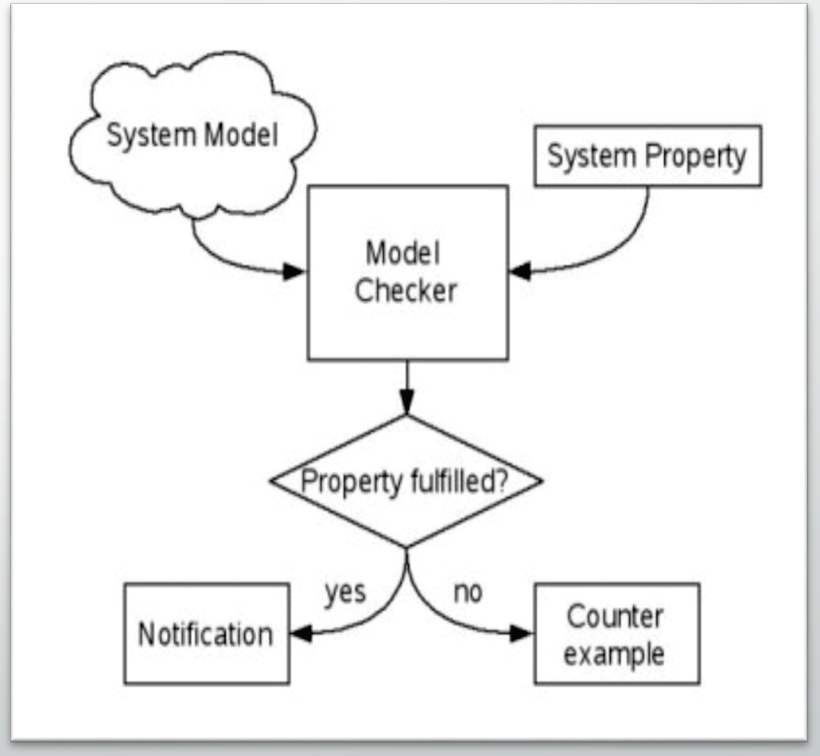


Fig.4 : Diagramma di funzionamento di un model checker

Metodo usato

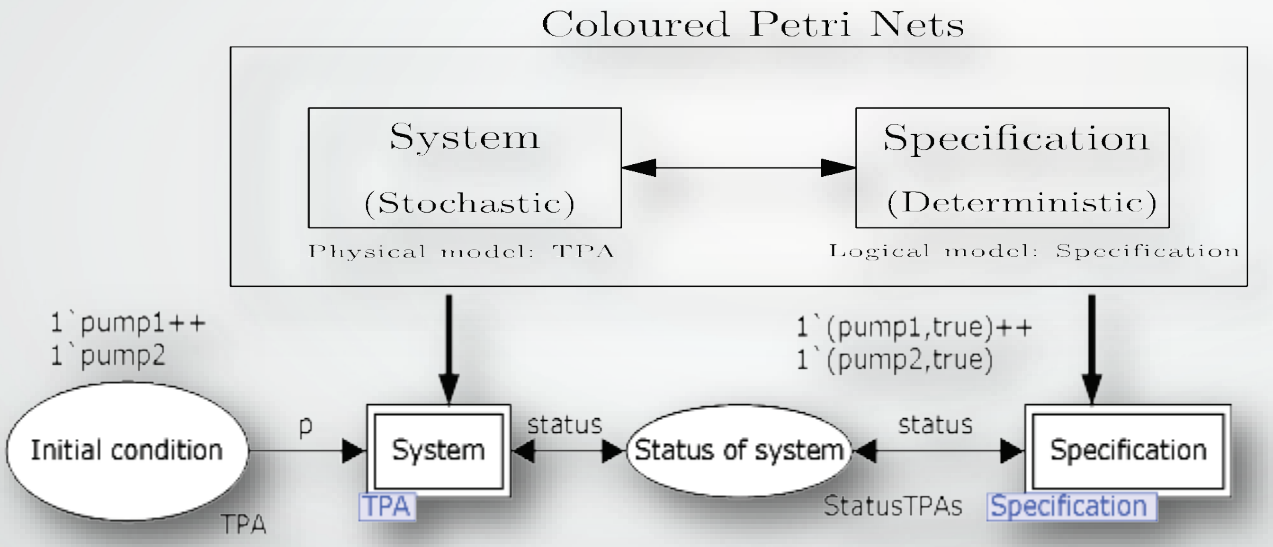
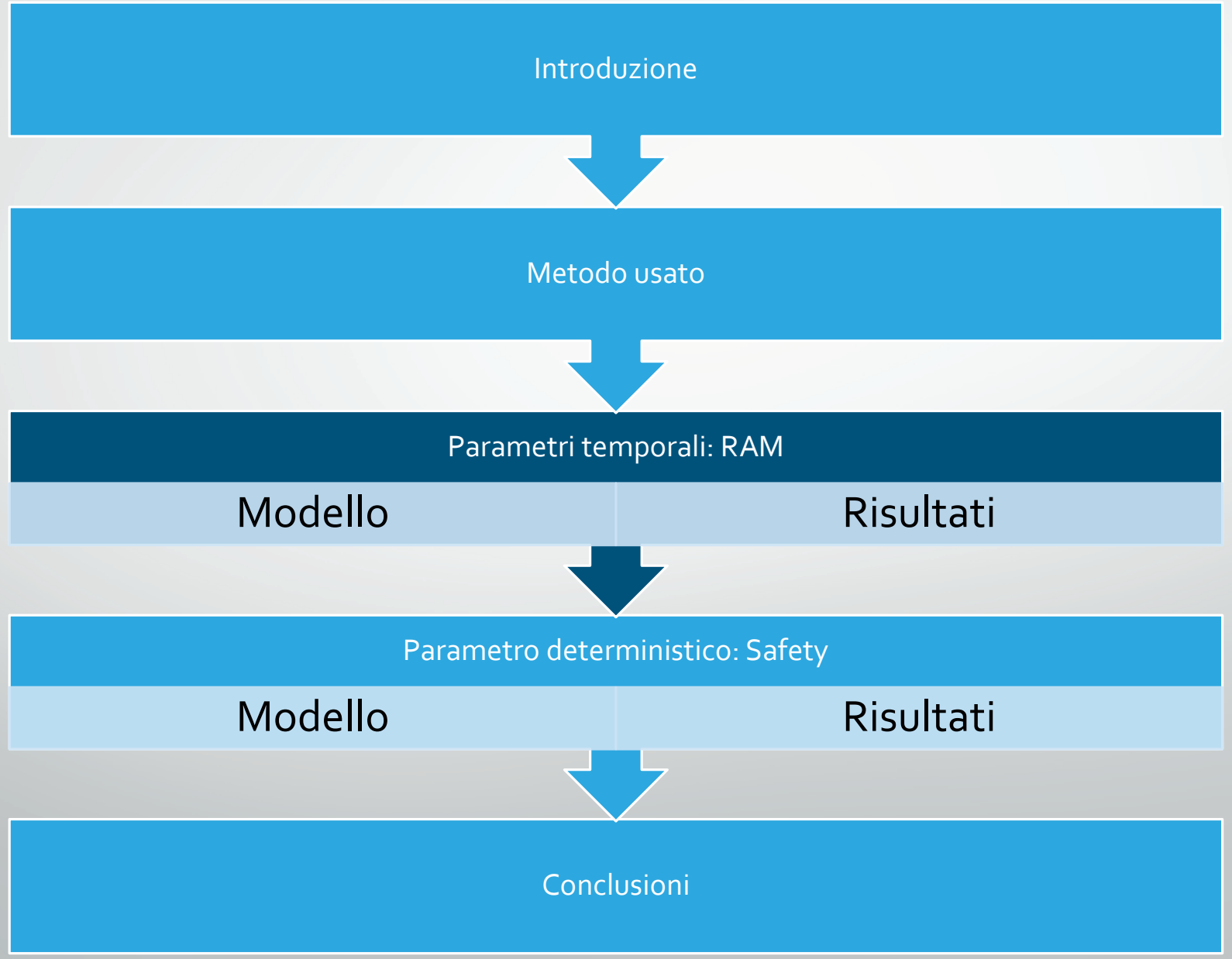


Fig.5: Rappresentazione gerarchica del sistema modellato

Outline


Introduzione
Metodo usato
Parametri temporali: RAM
Modello
Risultati
Parametro deterministico: Safety
Modello
Risultati
Conclusioni

RAM – Modello fisico

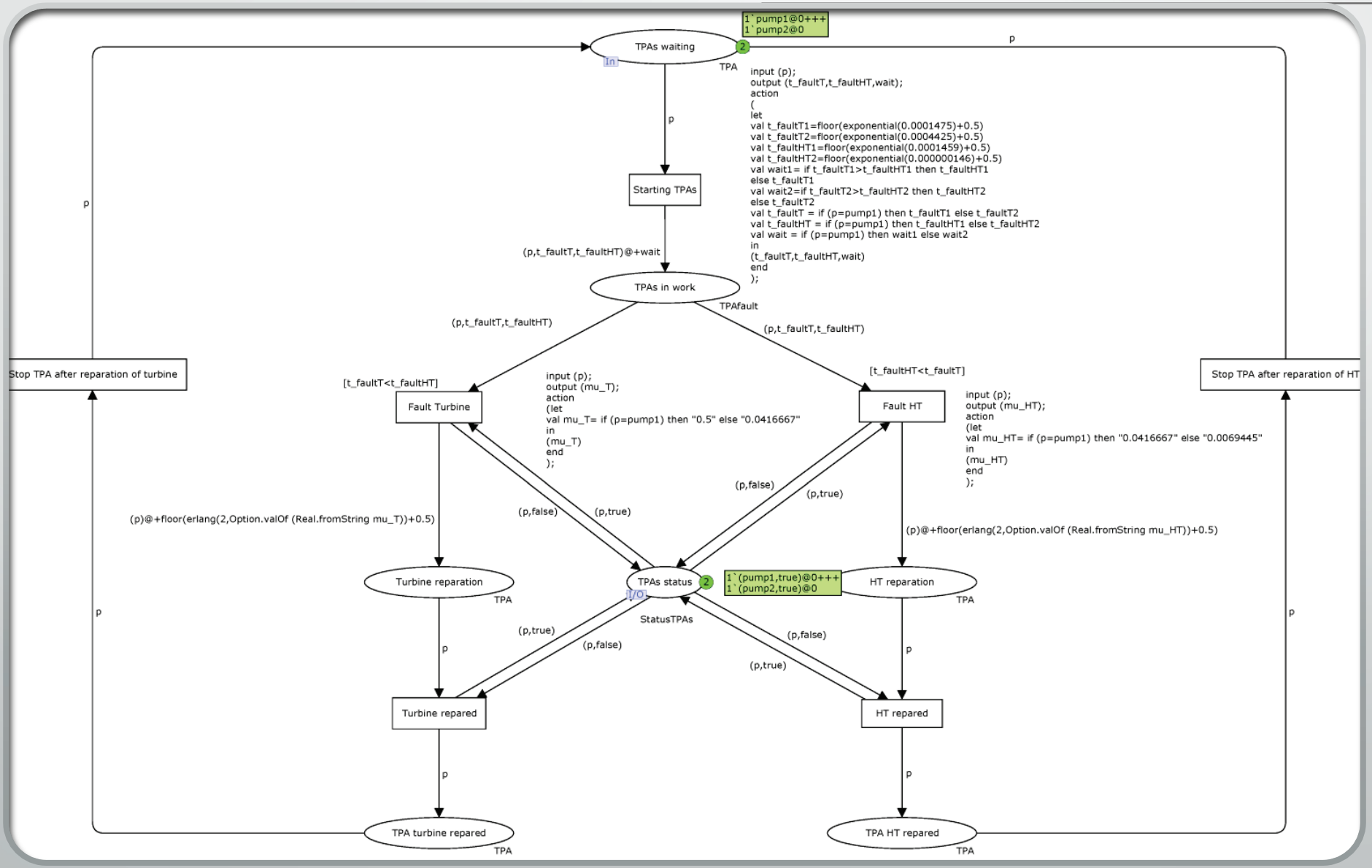


Fig.6: Rete di Petri Colorata, modello fisico

RAM – Modello fisico, dettagli

Calcolo guasto

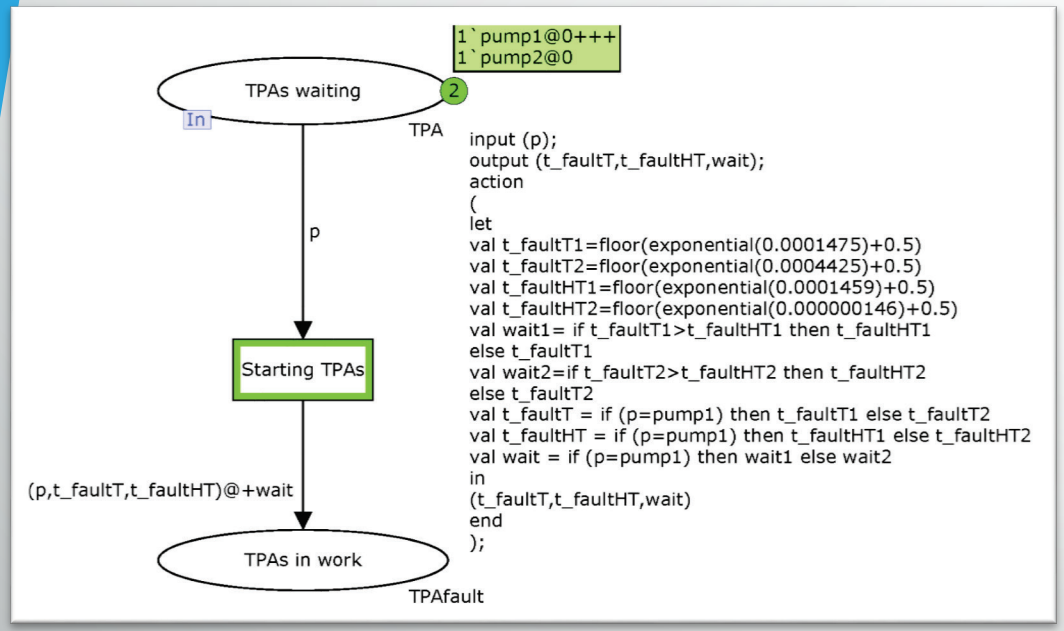


Fig.7: Particolare del modello fisico, avvio.

Calcolo riparazione

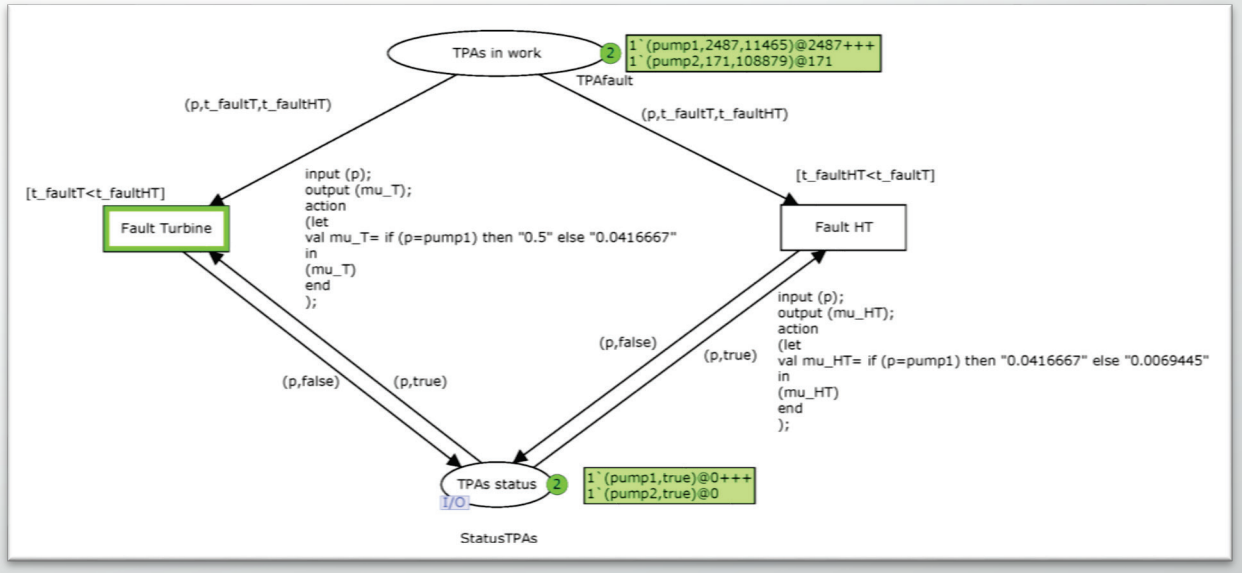


Fig.8: Particolare del modello fisico, guasto.

RAM – Modello fisico

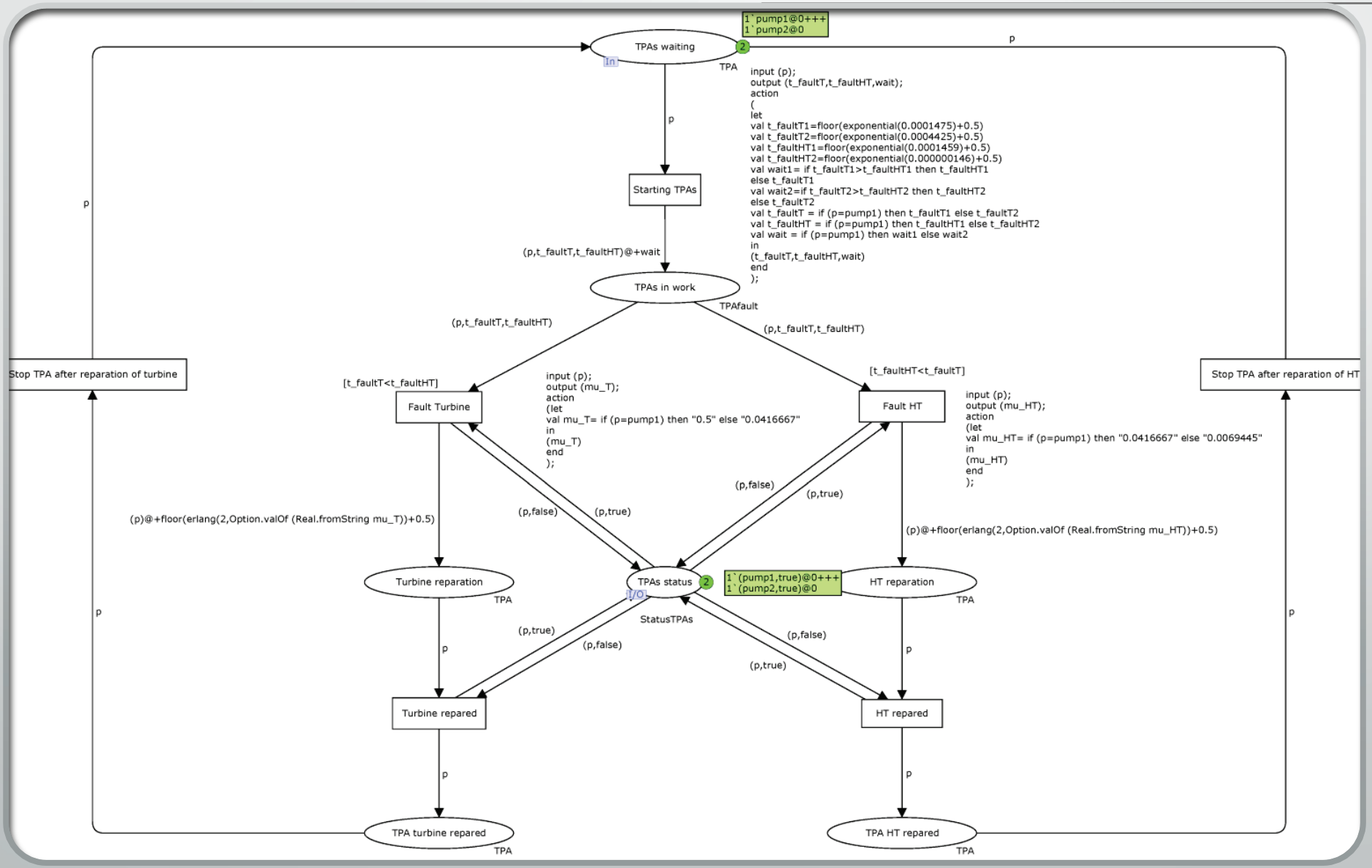


Fig.6: Rete di Petri Colorata, modello fisico

RAM – Modello del controllo

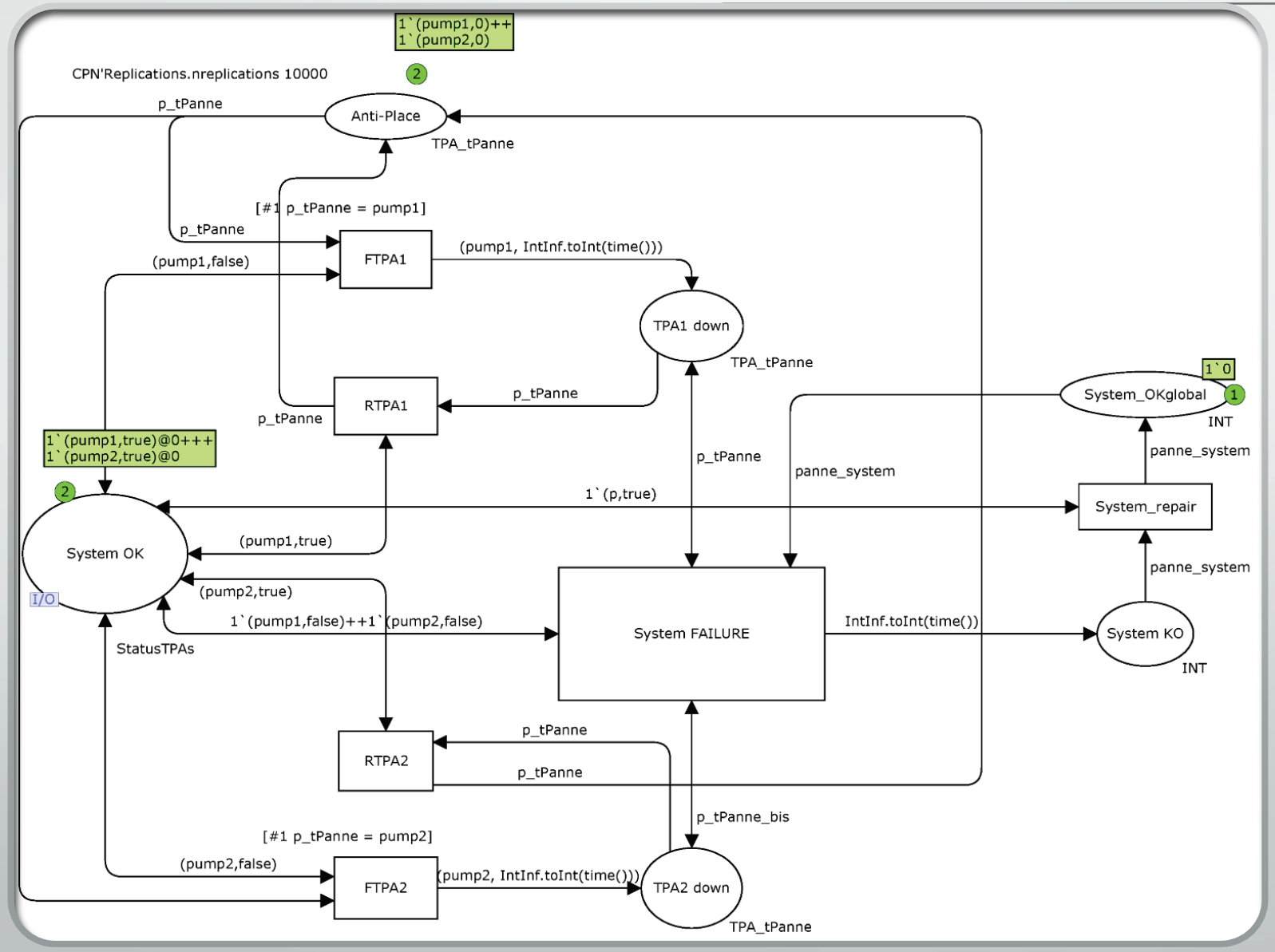
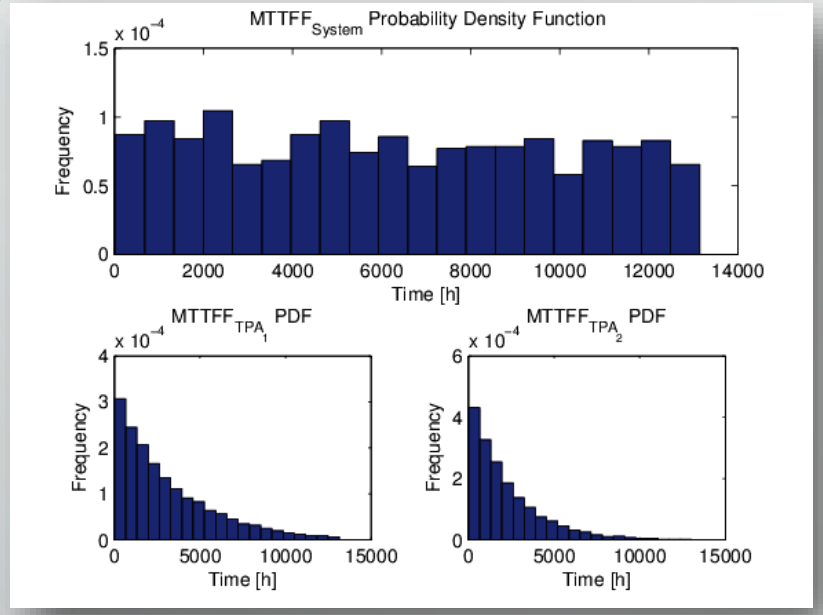


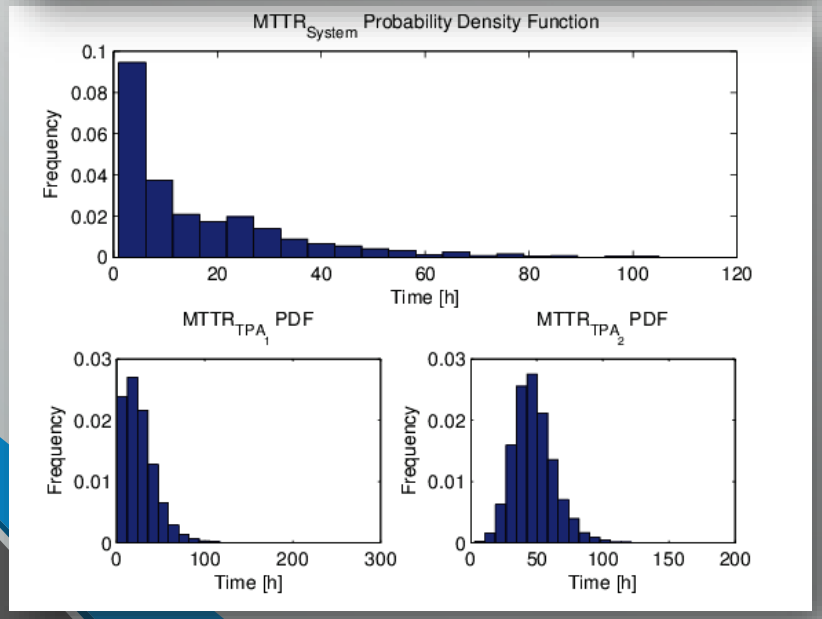
Fig.9: Rete di Petri Colorata, modello del controllo

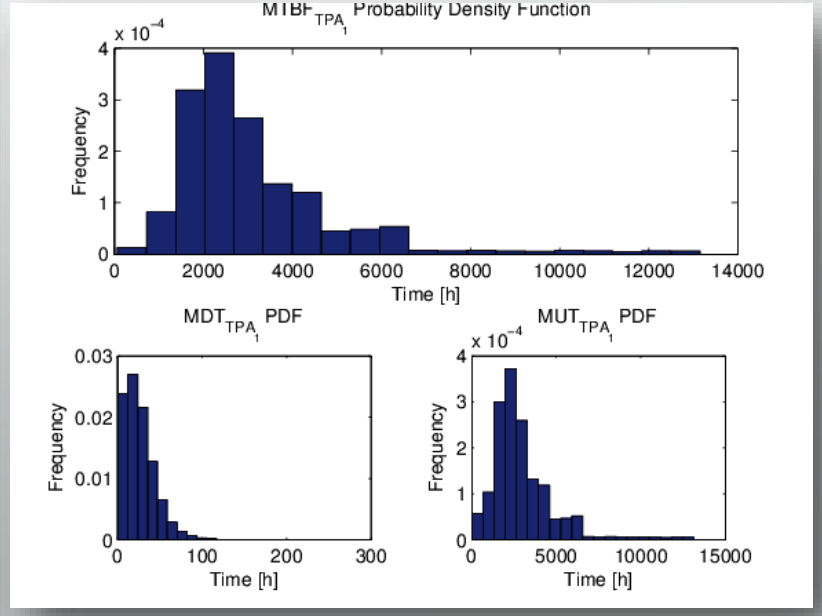
RAM - Risultati



Entità	MTTFF [h]	MTBF [h]	MTTR [h]	MUT [h]	MDT [h]
TPA_1	3111.7	3144.2	26.4	3020.1	26.4
TPA_2	2235.2	2259.2	48	2135.9	48
Sistema	6340.5	6312.8	16.4	6290.9	16.4

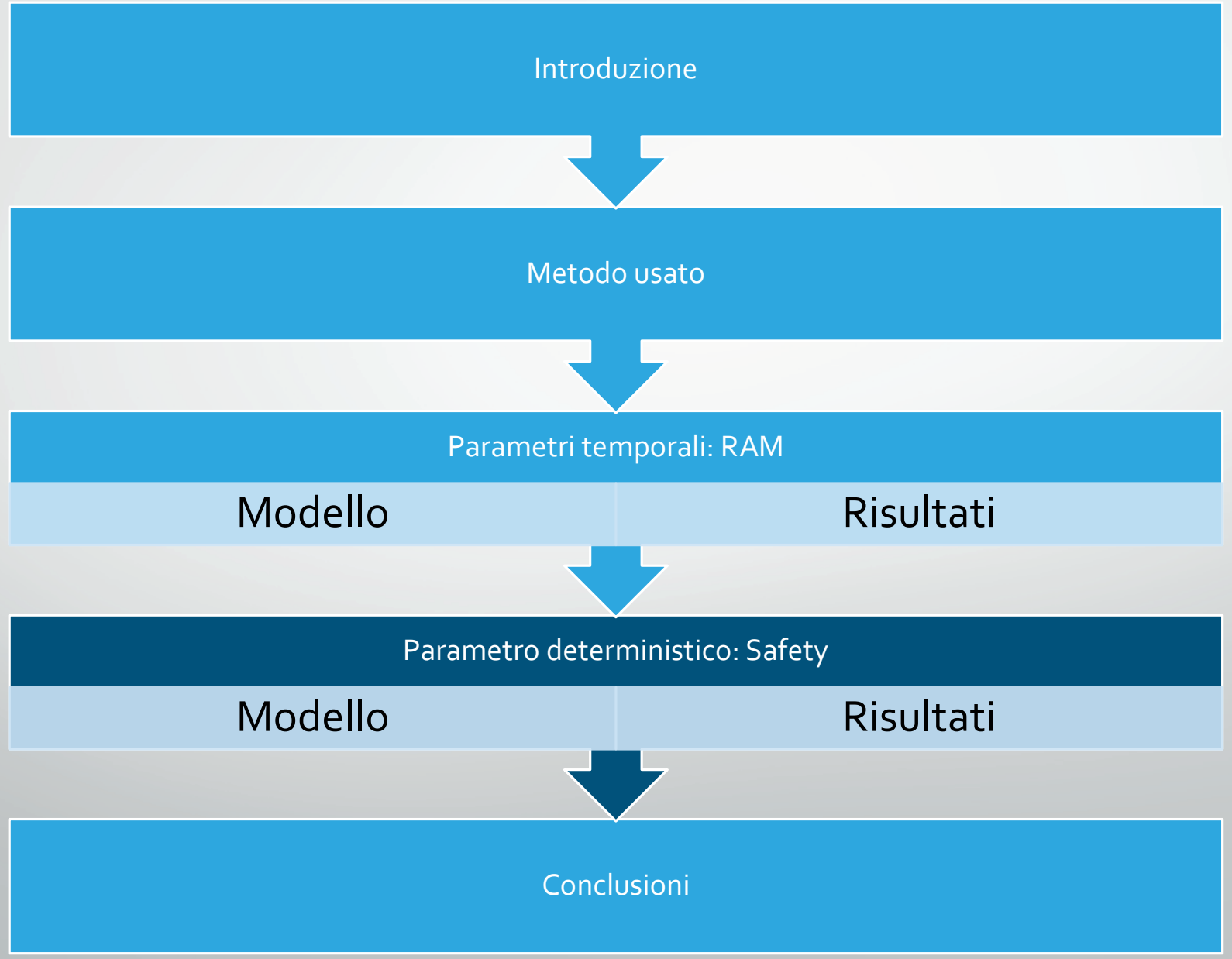
Tab.2: Risultati prestazionali





Varie figure, in alto a sinistra MTTFF, sotto MTTR, ed accanto un particolare della TPA_1

Outline


Introduzione
Metodo usato
Parametri temporali: RAM
Modello
Risultati
Parametro deterministico: Safety
Modello
Risultati
Conclusioni

Safety – Modello fisico

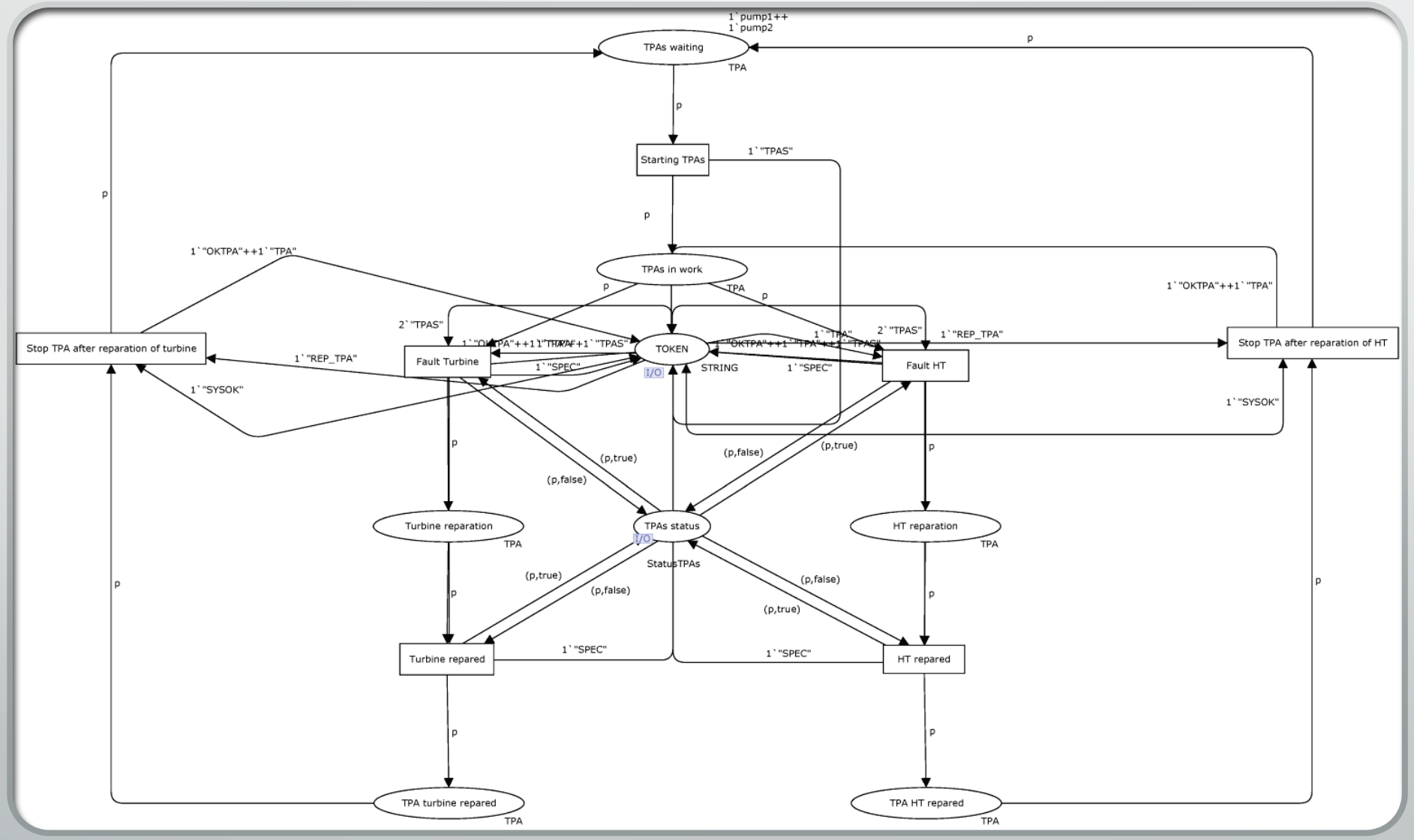


Fig.10: Rete di Petri Colorata deterministica, modello fisico

Safety – Modello del controllo

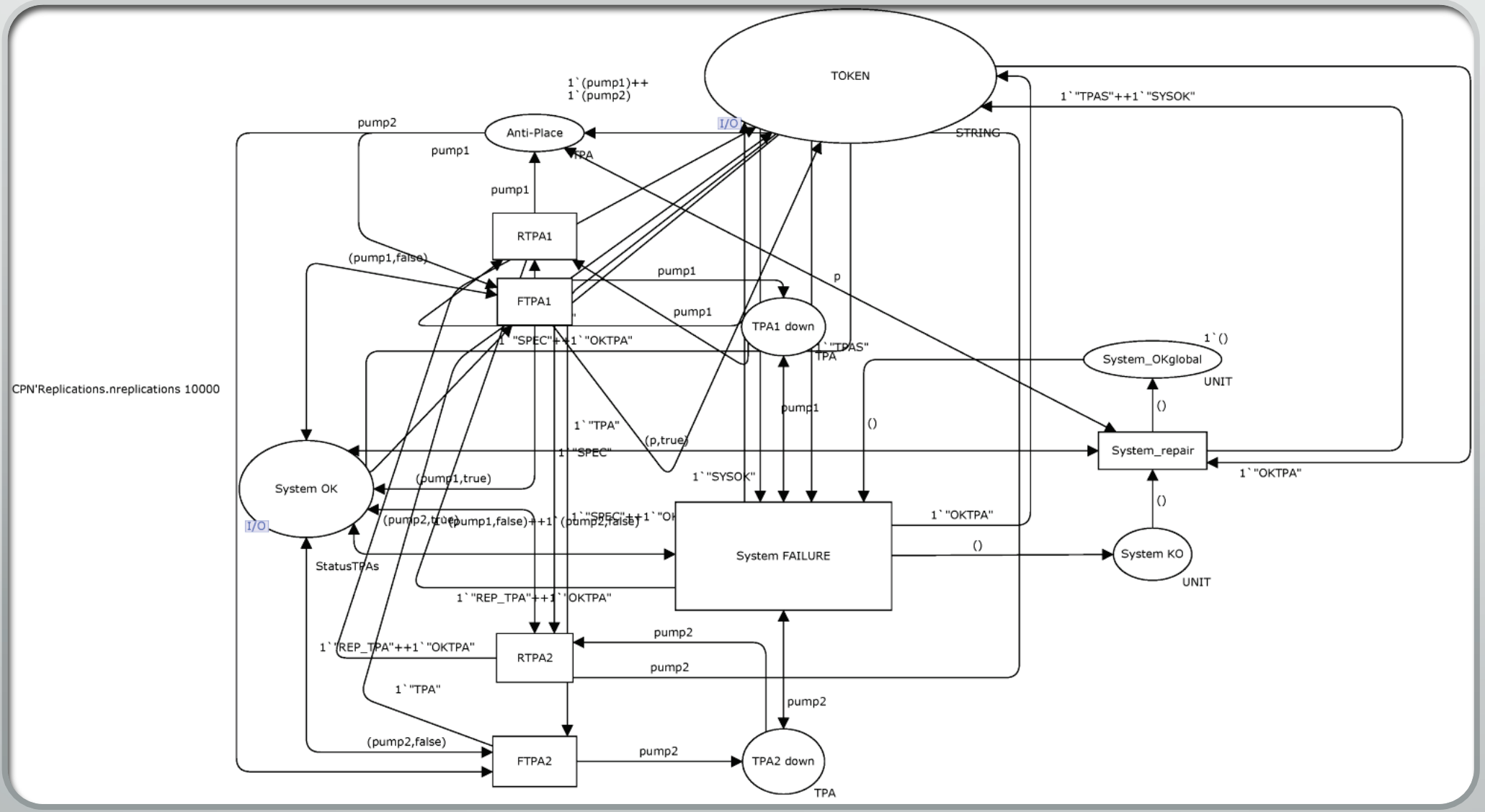


Fig.11: Rete di Petri Colorata deterministica, modello del controllo

Safety - Risultati

Spazio di stato :
72 nodi
100 archi

Formal model verification

CPN Tools

Old state space tool

Pros

- Implemented in CPN Tools GUI
- State space graph
- Text report
- CTL implemented
- Manual and support exist

Cons

- No LTL implementation
- Limited CTL
- Difficult exploration of the state space

New state space tool (ASAP)

Pros

- LTL Model Checking
- Faster generation of state space
- State reduction techniques

Cons

- No GUI, no state space graph
- No documentation, limited support
- Uncommented source code
- SML code difficult to understand

ProM - Process Mining workbench

Pros

- Import CPN models
- LTL model checking with timed model

Cons

- Model checking made by a simulation trace, thus cannot ensure if the entire state space is checked

Fig.12: Le tecniche usate per la verificazione

Safety – Risultati - ASAP

TOY

- 3 nodi
- 4 archi

```
val it =
 ((HT
    {eq_pred=fn,hash_fn=fn,n_items=ref 4,not_found=NotFound(-),
     table=ref
           (32,
            #[[|NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,
              NIL,
              B
               (0wx127733AF,
                (2,{toy_model={broken=[()],init=[],work=[]}}),(),
                B
                 (0wx169B642F,
                  (2,{toy_model={broken=[],init=[],work=[()]}}),(),
                  B
                   (0wx16BB84AF,
                    (2,{toy_model={broken=[],init=[()],work=[]}}),(),
                    NIL))),
              B
               (0wx169B6430,
                (3,{toy_model={broken=[],init=[],work=[()]}}),(),NIL),
              NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,NIL,
              NIL|]]}},()),(),())
 : unit MyDFSTraceExploration.storage * unit * unit
```

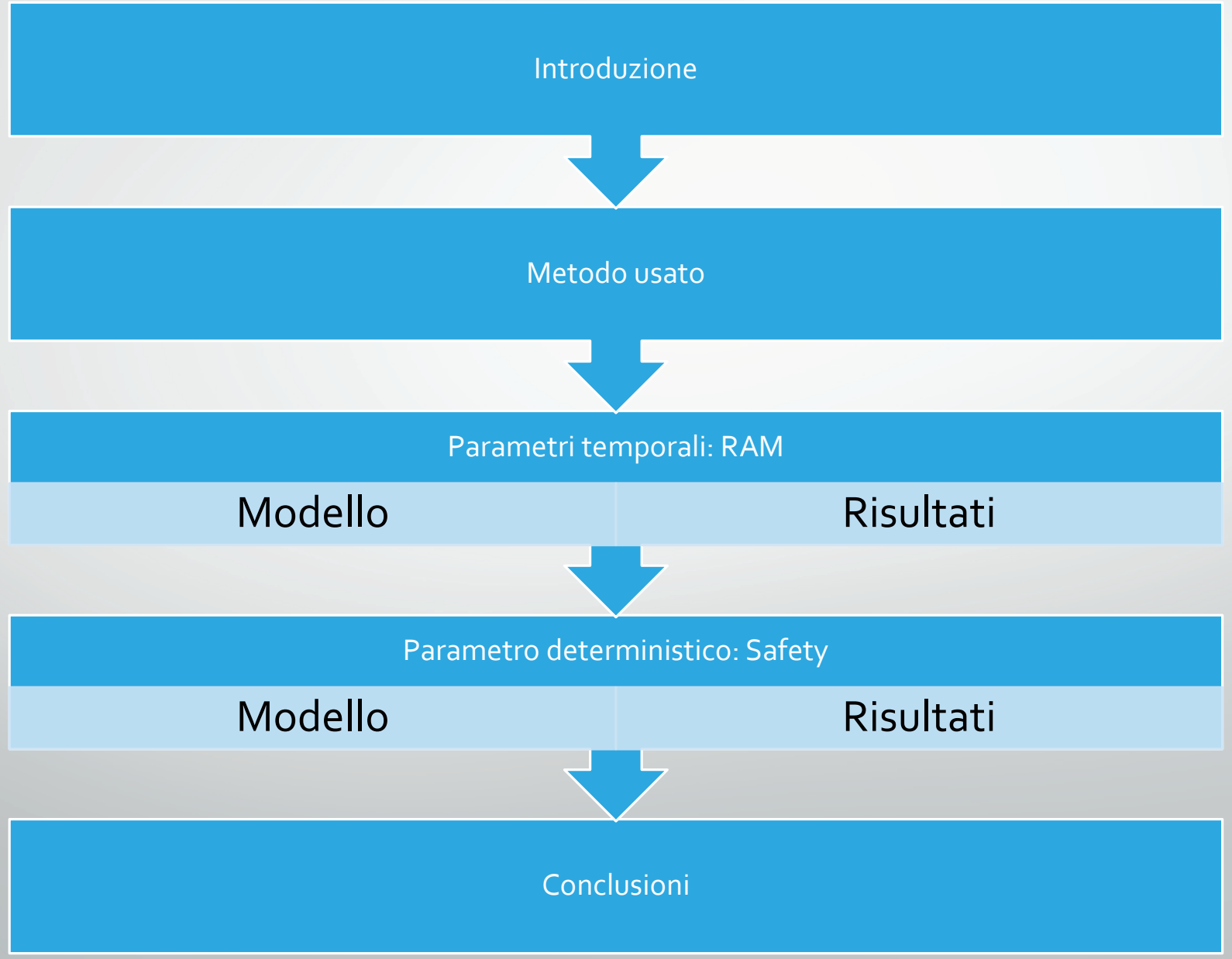
In figura, risultati di query in CPN Tool con ASAP

MODELLO

- 72 nodi
- 100 archi

```
                "TPAS"]}}),(),NIL),NIL,NIL,NIL,
          B
           (0wx79E86D62,
            (2,
             {Top={Specification={Anti=[pump2],System_KO=[()],
                                 System_OKglobal=[],
                                 TPA1_down=[pump1],TPA2_down=[]},
                   Status_of_system=[(pump1,false),(pump2,true)],
                   System={HT_reparation=[],TPA_HT_repared=[],
                           TPA_turbine_repared=[pump2],
                           TPAs_in_work=[],TPAs_waiting=[],
                           Turbine_reparation=[pump1]},
                   TOKEN=["OKTPA","REP_TPA"]}}),(),
            B
             (0wx44A26E2,
              (2,
               {Top={Specification={Anti=[pump2],System_KO=[],
                                   System_OKglobal=[()],
                                   TPA1_down=[pump1],TPA2_down=[]},
                     Status_of_system=[(pump1,false),(pump2,false)],
                     System={HT_reparation=[pump1],
                             TPA_HT_repared=[],
                             TPA_turbine_repared=[],
                             TPAs_in_work=[],TPAs_waiting=[],
                             Turbine_reparation=[pump2]},
                     TOKEN=["OKTPA","SPEC","SYSOK","TPAS","TPAS"]}}),
              (),
              B
               (0wx16625D62,
                (2,
                 {Top={Specification={Anti=[pump1],System_KO=[()],
                                     System_OKglobal=[],
                                     TPA1_down=[],
                                     TPA2_down=[pump2]},
                       Status_of_system=[(pump2,false),
                                         (pump1,true)],
                       System={HT_reparation=[pump2],
                               TPA_HT_repared=[],
                               TPA_turbine_repared=[pump1],
                               TPAs_in_work=[],TPAs_waiting=[],
                               Turbine_reparation=[]},
                       TOKEN=["OKTPA","REP_TPA"]}}),(),NIL))),
          NIL,...|]]}},()),(),())
: unit MyDFSTraceExploration.storage * unit * unit
```

Outline


Introduzione
Metodo usato
Parametri temporali: RAM
Modello
Risultati
Parametro deterministico: Safety
Modello
Risultati
Conclusioni

Conclusioni

RAM

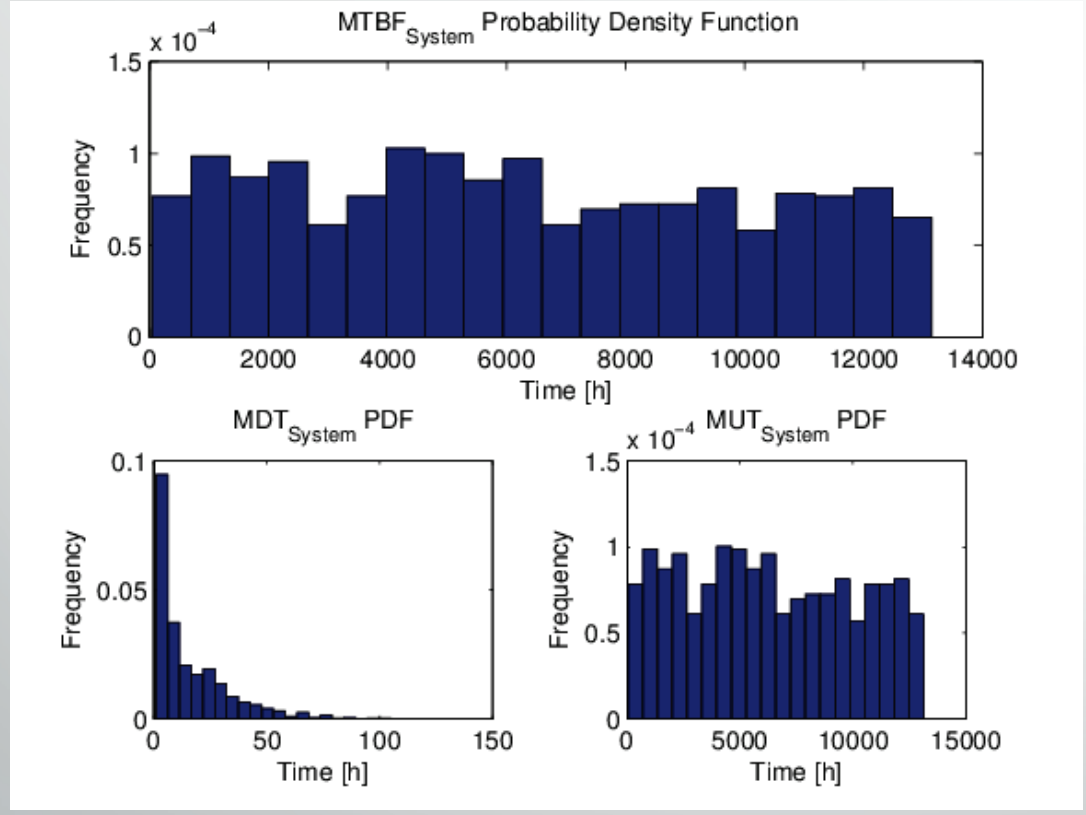


Fig.13: PDF del sistema

Safety

```
                    "TPAS"]}}),(),NIL),NIL,NIL,NIL,
              B
               (0wx79E86D62,
                (2,
                 {Top={Specification={Anti=[pump2],System_KO=[()],
                                     System_OKglobal=[],
                                     TPA1_down=[pump1],TPA2_down=[]},
                       Status_of_system=[(pump1,false),(pump2,true)],
                       System={HT_reparation=[],TPA_HT_repared=[],
                               TPA_turbine_repared=[pump2],
                               TPAs_in_work=[],TPAs_waiting=[],
                               Turbine_reparation=[pump1]},
                       TOKEN=["OKTPA","REP_TPA"]}}),(),
                B
                 (0wx44A26E2,
                  (2,
                   {Top={Specification={Anti=[pump2],System_KO=[],
                                       System_OKglobal=[()],
                                       TPA1_down=[pump1],TPA2_down=[]},
                         Status_of_system=[(pump1,false),(pump2,false)],
                         System={HT_reparation=[pump1],
                                 TPA_HT_repared=[],
                                 TPA_turbine_repared=[],
                                 TPAs_in_work=[],TPAs_waiting=[],
                                 Turbine_reparation=[pump2]},
                         TOKEN=["OKTPA","SPEC","SYSOK","TPAS","TPAS"]}}),
                  (),
                  B
                   (0wx16625D62,
                    (2,
                     {Top={Specification={Anti=[pump1],System_KO=[()],
                                         System_OKglobal=[],
                                         TPA1_down=[],
                                         TPA2_down=[pump2]},
                           Status_of_system=[(pump2,false),
                                             (pump1,true)],
                           System={HT_reparation=[pump2],
                                   TPA_HT_repared=[],
                                   TPA_turbine_repared=[pump1],
                                   TPAs_in_work=[],TPAs_waiting=[],
                                   Turbine_reparation=[]},
                           TOKEN=["OKTPA","REP_TPA"]}}),(),NIL))),
                    NIL,...|]]}},()),(),())
: unit MyDFSTraceExploration.storage * unit * unit
```

Fig.14: Risultato query con ASAP

Don’t watch the clock; do what it does. Keep going.

Sam Levenson