Tecniche Intelligenti di Fault Detection, Identification e Recovery

Luigi Portinale, Daniele Codetta Raiteri

Computer Science Institute

University of Piemonte Orientale "A. Avogadro"

Alessandria (Italy)

POLOICT

Dipartimento di Informatica

AMEDEO AVOGADRO università degli studi del piemonte orientale

Chi siamo

- Istituto di Informatica (Dip. Scienze e Innov. Tecnologica)
  - Precedentemente Dipartimento di Informatica
- 17 docenti e ricercatori attivi nelle seguenti aree e laboratori
  - *Intelligenza Artificiale (Sistemi Intelligenti di Supporto alle Decisioni, Machine Learning e Data Mining)*
  - *Modelli ed Analisi Quantitativa (Reliability, Performance Evaluation)*
  - *Cloud e Distributed Computing*
  - *Bioinformatica*
  - *Informatica medica (e-health)*
- 1 spin-off Penta solutions (*domotica*)
- 1 laboratorio di Technology Enhanced Learning

Giovedì, 10 Maggio 2012 Cerca: Enter Search... Invia

Dipartimento di Informatica

Università del Piemonte Orientale "Amedeo Avogadro" - Alessandria, Novara e Vercelli

Ateneo | Facoltà di Scienze M.F.N. | Cercapersone | Link | Trasparenza | Mappa del Sito

Home

- Chi siamo
- Dove siamo
- Organizzazione - Personale
- Ricerca
- Pubblicazioni
- Didattica
- Dottorato di Ricerca
- Bandi e concorsi
- Trasparenza e Bilanci
- Link utili
- Servizi
- Eventi

Ultime notizie

Avviso Seminario Polo ICT
Tecniche Intelligenti di FDIR (Fault Detection, Identification and Recovery).

Continua... - *11/04/2012* - *Scadenza: 15/05/2012*

Archivio notizie...

Ultime pubblicazioni

- Quantification of Dependencies between Electrical and Information Infrastructures
  Marco Beccuti, Silvano Chiaradonna, Felicita Di Giandomenico, Susanna Donatelli, Giovanna Dondossola, Giuliana Franceschinis 2012
- Minimum pattern length for short spaced seeds based on linear rulers
  Lavinia Egidi, Giovanni Manzini 2012
- Reasoning about actions with Temporal Answer Sets
  Laura Giordano, Alberto Martelli, Daniele Theseider Dupré 2012

Archivio pubblicazioni...

www[at]di.unipmn.it

Dipartimento di Informatica - Università del Piemonte Orientale "A. Avogadro"
viale Teresa Michel, 11 - 15121 - Alessandria
Partita IVA 01943490027 - C.F. 94021400026

Sommario

- Dependability, Reliability e FDIR
- Probabilistic Graphical Models (BN and DBN)
  - Reti Bayesiane (Bayesian Networks)
  - Reti Bayesiane Dinamiche (Dynamic Bayesian Networks)
- Dalla Fault Tree Analysis ai modelli grafico-probabilistici
- Case Studies
  - 3ASI Benchmark
  - Cascading failures in a power grid
  - Autonomous FDIR in a mars rover
- Tools
- Open Issues

Sommario

- Dependability, Reliability e FDIR
- Probabilistic Graphical Models (BN and DBN)
  - Reti Bayesiane (Bayesian Networks)
  - Reti Bayesiane Dinamiche (Dynamic Bayesian Networks)
- Dalla Fault Tree Analysis ai modelli grafico-probabilistici
- Case Studies
  - 3ASI Benchmark
  - Cascading failures in a power grid
  - Autonomous FDIR in a mars rover
- Tools
- Open Issues

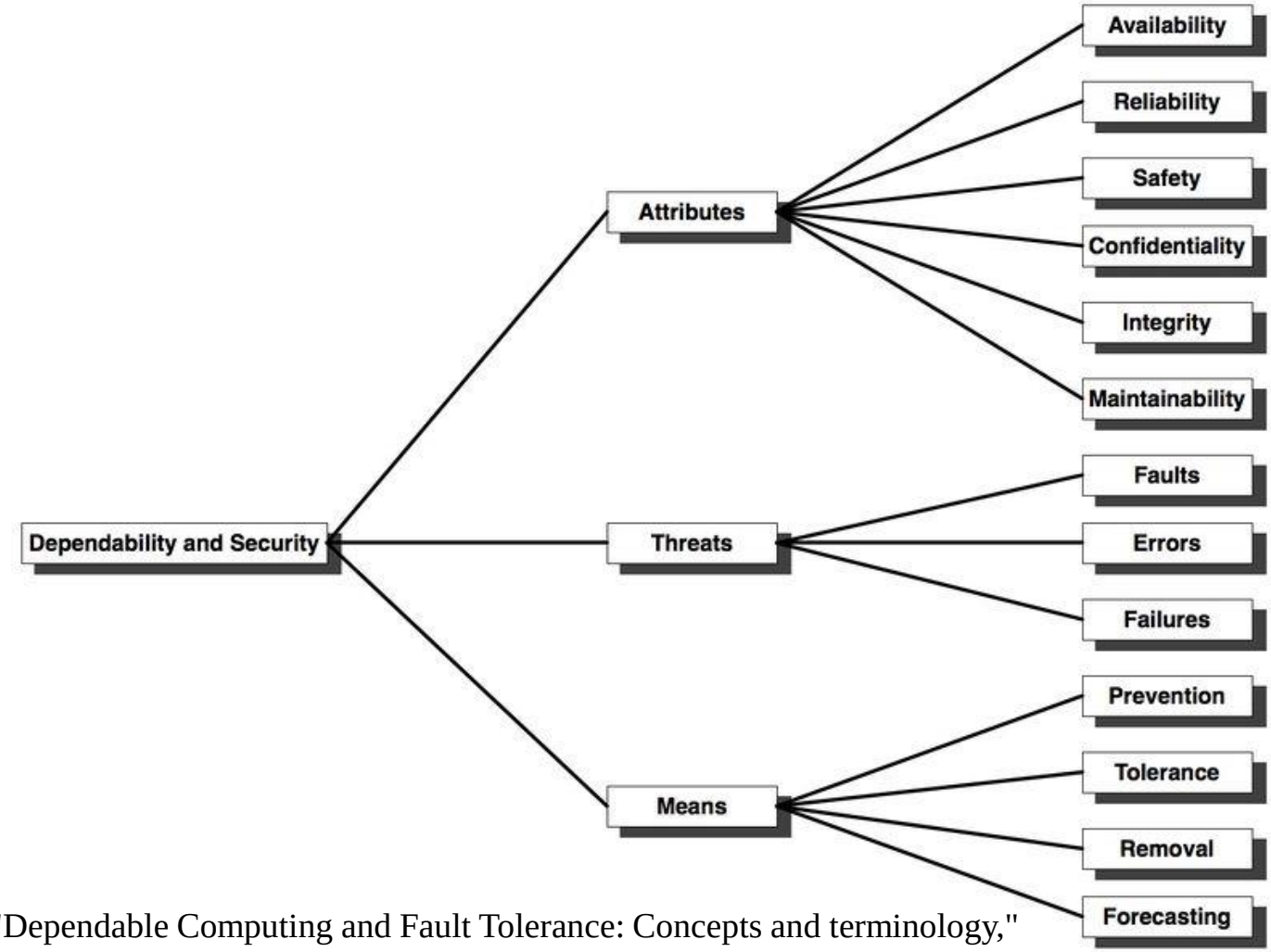
Dependability vs Reliability

Si usa il termine dependability per identificare la capacita' di un sistema di poter fornire un servizio affidabile e su cui poter contare (trusted).

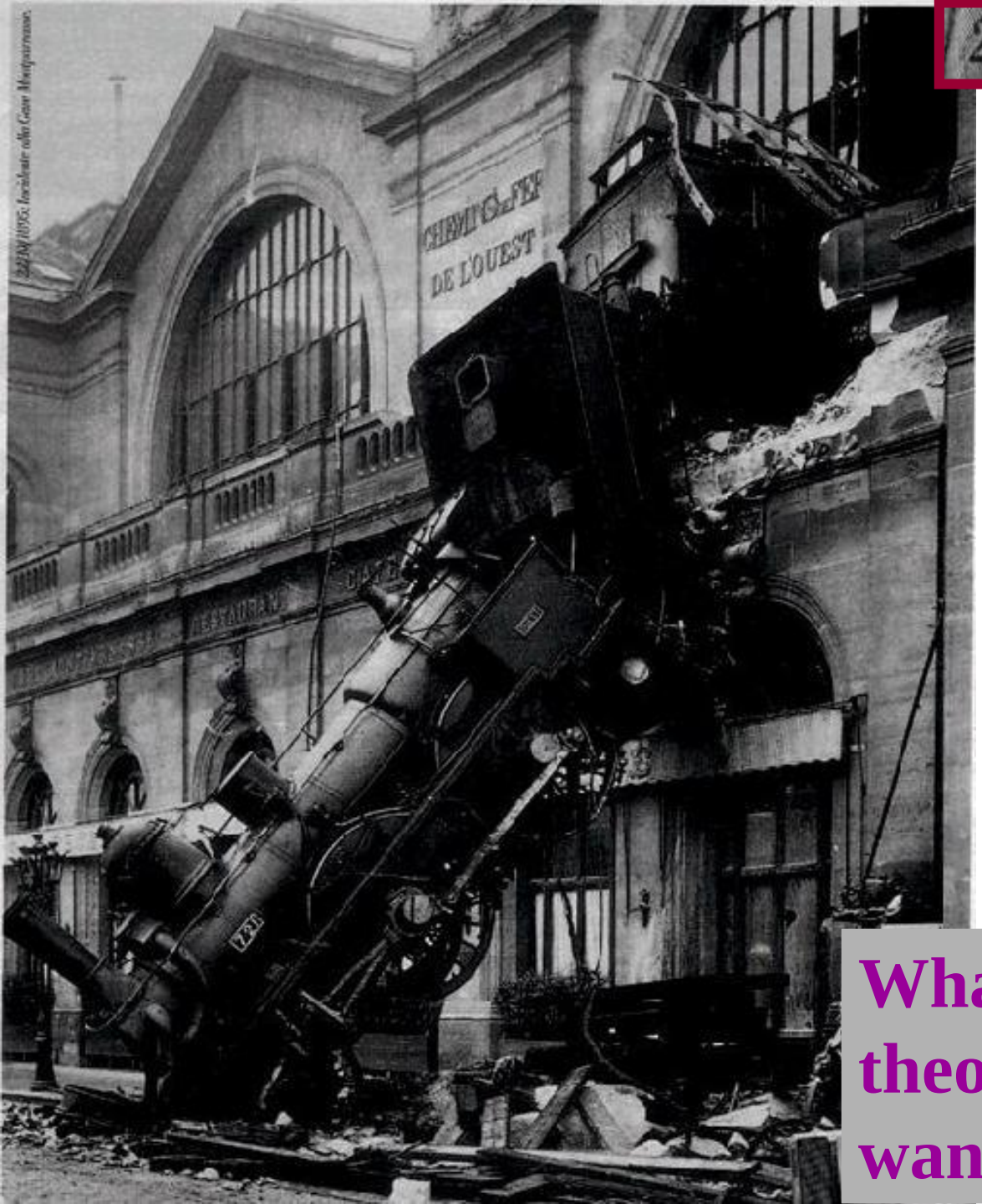
Dependability e' un concetto integrato di vari aspetti

- **Reliability**: continuita' di servizio corretto.
- **Availability**: disponibilita' di servizio corretto.
- **Maintainability**: capacita' di poter sostenere modifiche e riparazioni.
- **Safety**: assenza di conseguenze catastrofiche.
- (**Security**)

Dep/Sec Taxonomy



J.C. Laprie. "Dependable Computing and Fault Tolerance: Concepts and terminology," in Proc. 15th IEEE Int. Symp. on Fault-Tolerant Computing, 1985



22/10/1895: Gare Montparnasse.

What dependability theory and practice wants to avoid

Are these connections reliable ?

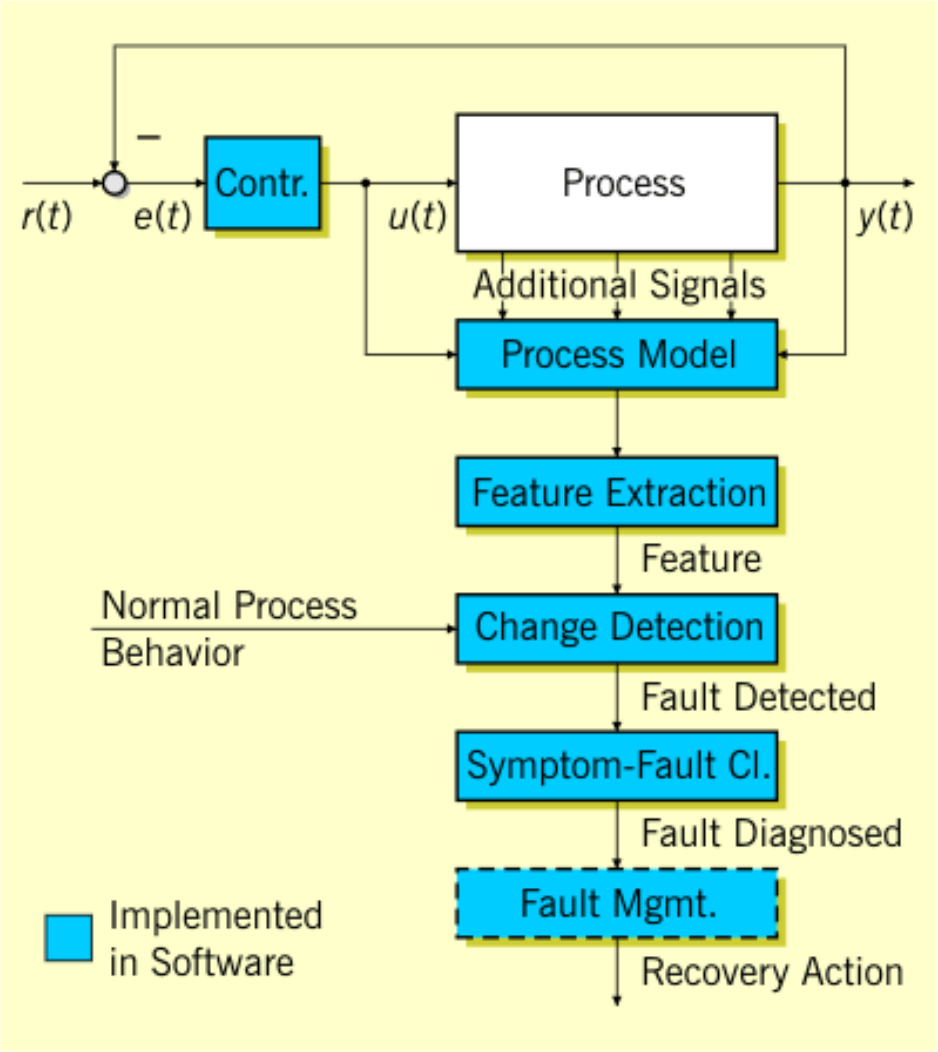
Qualche aspetto tecnico….

- **Failure**: una deviazione a livello di sistema dal comportamento corretto/atteso (*failure modes*)
- **Fault**: una causa di failure (un difetto nel sistema)
- **Error**: discrepanza tra comportamento atteso e comportamento osservato di una componente di sistema.
- **Fault-Error-Failure chain:** un fault, quando attivato, puo' portare ad un errore (invalid state) e lo stato non valido generato dall'errore puo' portare ad un altro errore o ad una failure (deviazione osservabile dal comportamento specificato per l'intero sistema)
- La catena puo' essere in effetti un loop (faults che causano failures, che causano altri faults, che causano altre failures, ecc…)

FDIR: nozioni di base

- **Fault Detection**: capacita' di scoprire la presenza di un guasto (deviazione parametri da valore nominale)
- **Fault Identification/Isolation (Diagnosi)**: capacita' di ascrivere il guasto ad una specifica componente e ad un suo specifico modo comportamentale (es: valveA stuck-on)
- **Fault Recovery**: capacita' di ripristinare la funzionalita' della componente guasta e/o eliminazione della causa del guasto

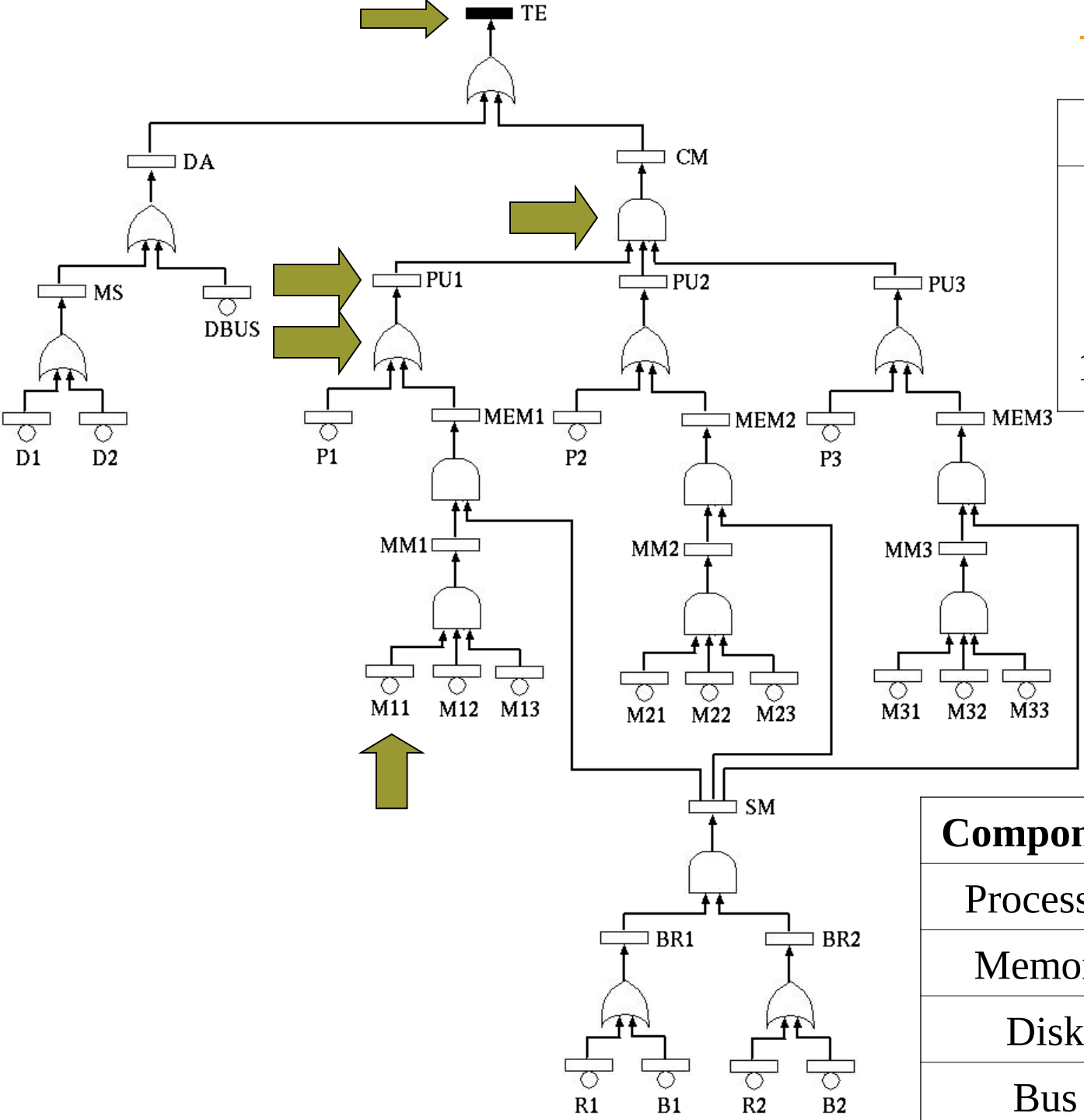
FDIR: modello generale



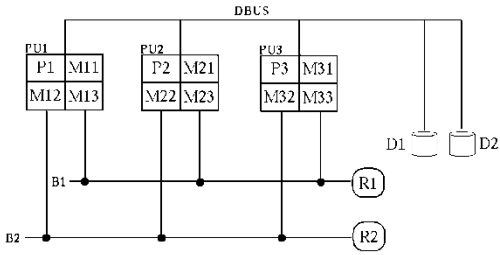
Un trend attuale…..

- Sfruttare modelli tipici dell'affidabilita' per approcciare il problema piu' generale di FDIR
- Intenso lavoro nel campo dell'Intelligenza Artificiale su tecniche e modelli per *"diagnosi intelligente"*
- Convergenza verso modelli grafico-probabilistici (Reti Bayesiane e derivati)

Fault Tree



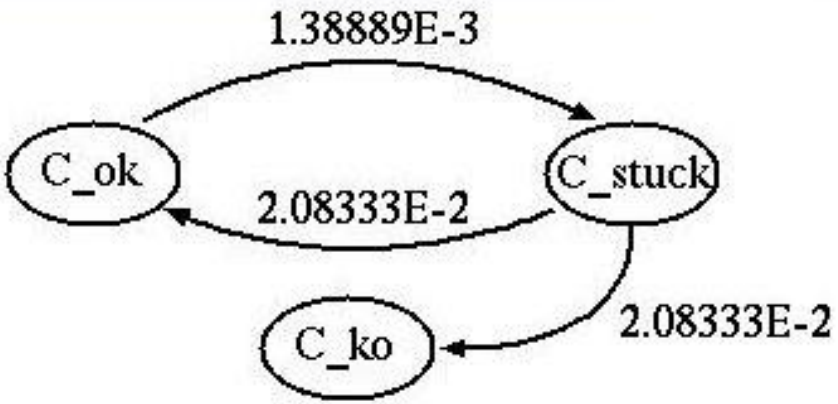
Time	Unreliability
4000 h	6.387520E-3
6000 h	9.565979E-3
8000 h	1.273428E-2
10000 h	1.589248E-2



Component	Failure rate (λ)
Processor	5.0E-7 1/h
Memory	3.0E-8 1/h
Disk	8.0E-7 1/h
Bus	2.0E-9 1/h

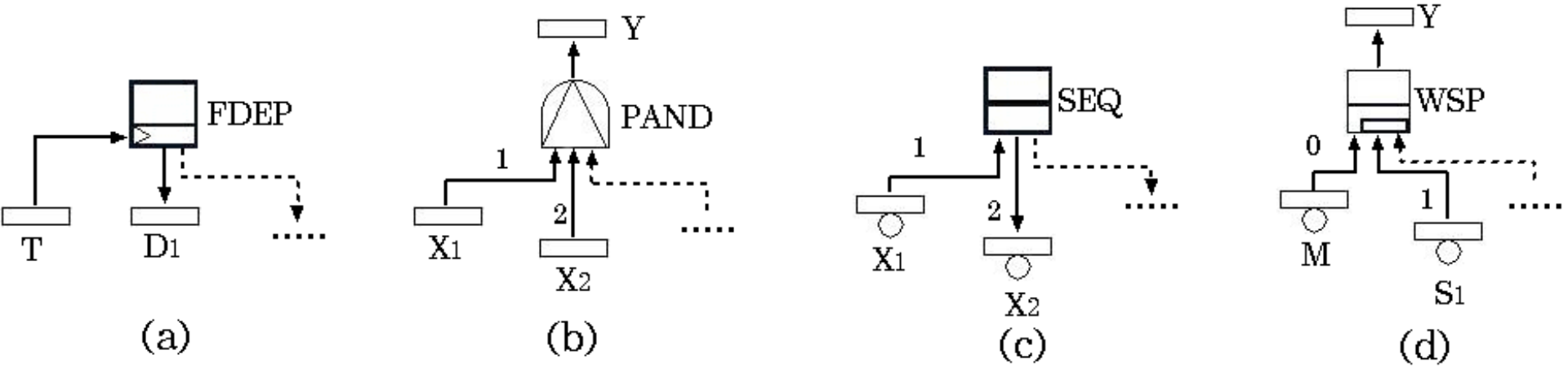
State Space Models

- Enumerazione degli stati di interesse del sistema e delle loro possibili transizioni.
  - **Markov Chains**, Markov Decision Processes, Petri Nets
  - Lo spazio degli stati puo' essere over-specified rispetto ai bisogni di analisi o modello
  - Il comportamento dinamico del sistema puo' portare all'esplosione dello spazio degli stati (size)



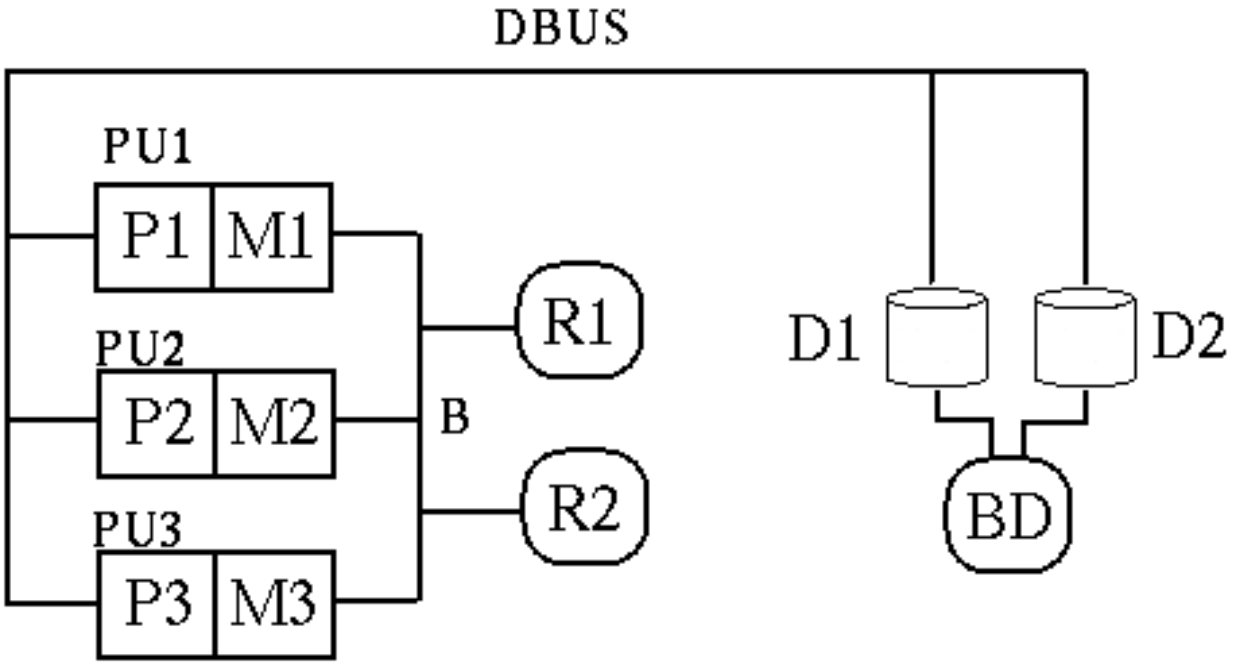
Local Dependencies: Dynamic Fault Trees

- Una dipendenza sorge quando il comportamento (anomalo) di una componente dipende dallo stato di altre componenti.
- DFTs catturano alcue dipendenze tramite i Gate Dinamici
  - Functional dependencies (FDEP gate)
  - Temporal dependencies (SEQ gate, PAND gate)
  - (Warm) spare components (WSP gate): multi-state components



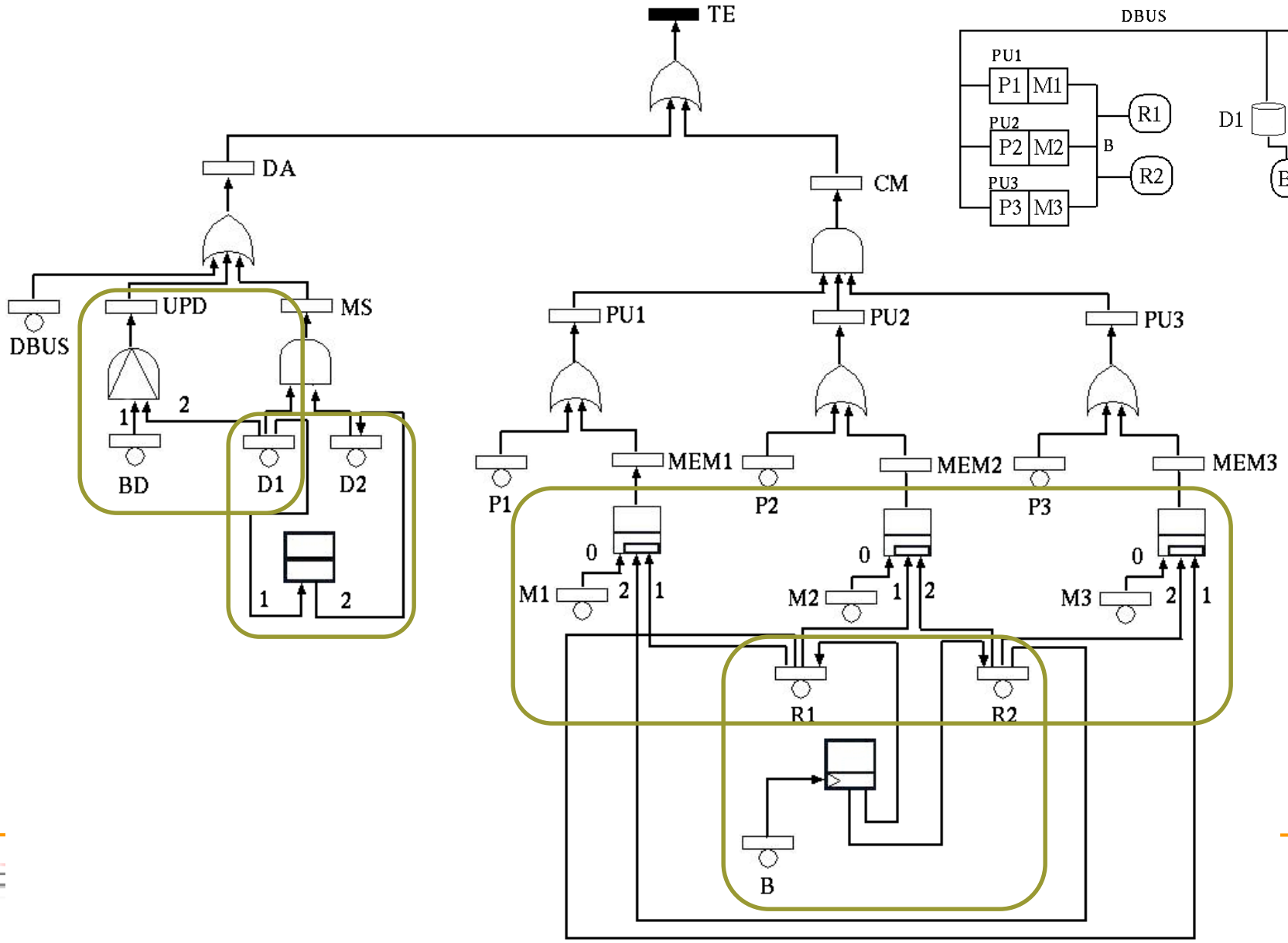
J. B. Dugan, S. J. Bavuso, M. A. Boyd, "Dynamic Fault-Tree Models for Fault-Tolerant Computer Systems", *IEEE Transactions on Reliability*, vol 41, 1992, pp 363-377

Esempio:
Multiprocessor Computing System



•R1 and R2 are warm spare memories. R1 and R2 functionally depend on the bus B.
•D1 is the primary disk; D2 is the backup disk. D2 can not fail before D1.
•BD is the device updating periodically D2. The failure of BD is relevant if it happens before the failure of D2.

Esempio: Dynamic FT



Sommario

- Dependability, Reliability e FDIR
- Probabilistic Graphical Models (BN and DBN)
  - Reti Bayesiane (Bayesian Networks)
  - Reti Bayesiane Dinamiche (Dynamic Bayesian Networks)
- Dalla Fault Tree Analysis ai modelli grafico-probabilistici
- Case Studies
  - 3ASI Benchmark
  - Cascading failures in a power grid
  - Autonomous FDIR in a mars rover
- Tools
- Open Issues

Probabilistic Graphical Models

- Modelli Statici
  - Bayesian Networks (aka Causal Networks, Probabilistic Networks, Belief Networks,…)
  - Influence Diagrams
- Modelli Dinamici
  - Dynamic Bayesian Networks (2TBN)
  - Dynamic Decision Networks

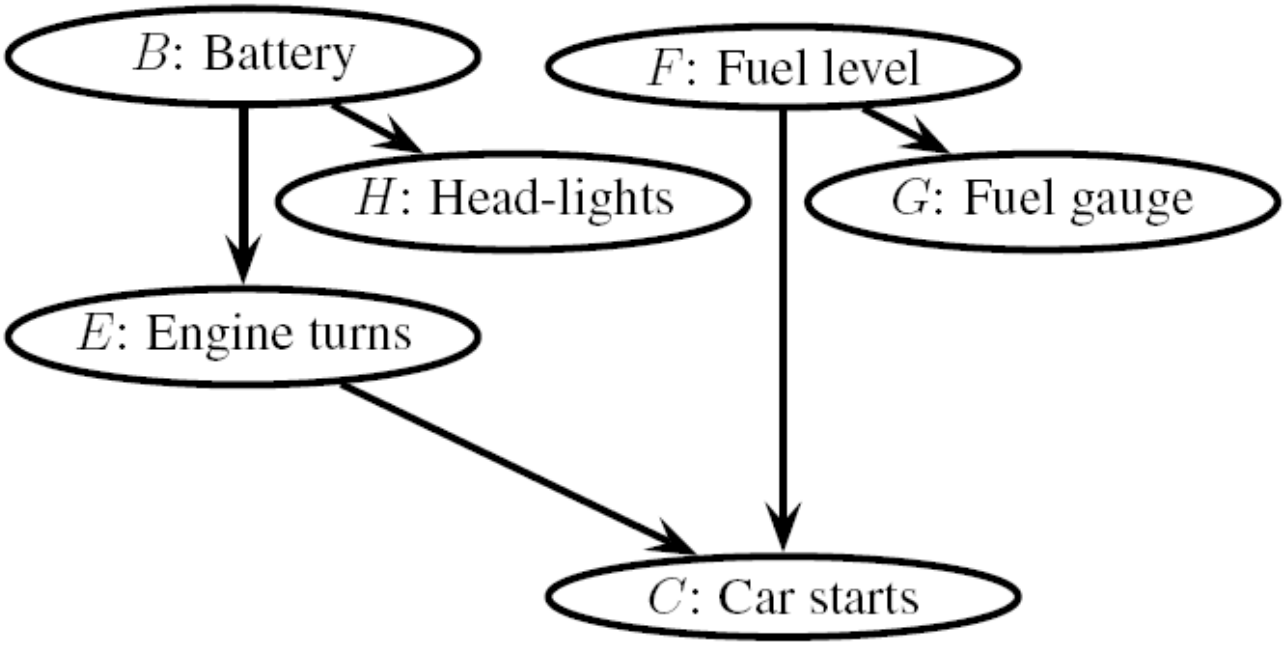
Probabilistic Graphical Models

- Modelli Statici
  - Bayesian Networks (aka Causal Networks, Probabilistic Networks, Belief Networks,…)
  - Influence Diagrams
- Modelli Dinamici
  - Dynamic Bayesian Networks (2TBN)
  - Dynamic Decision Networks

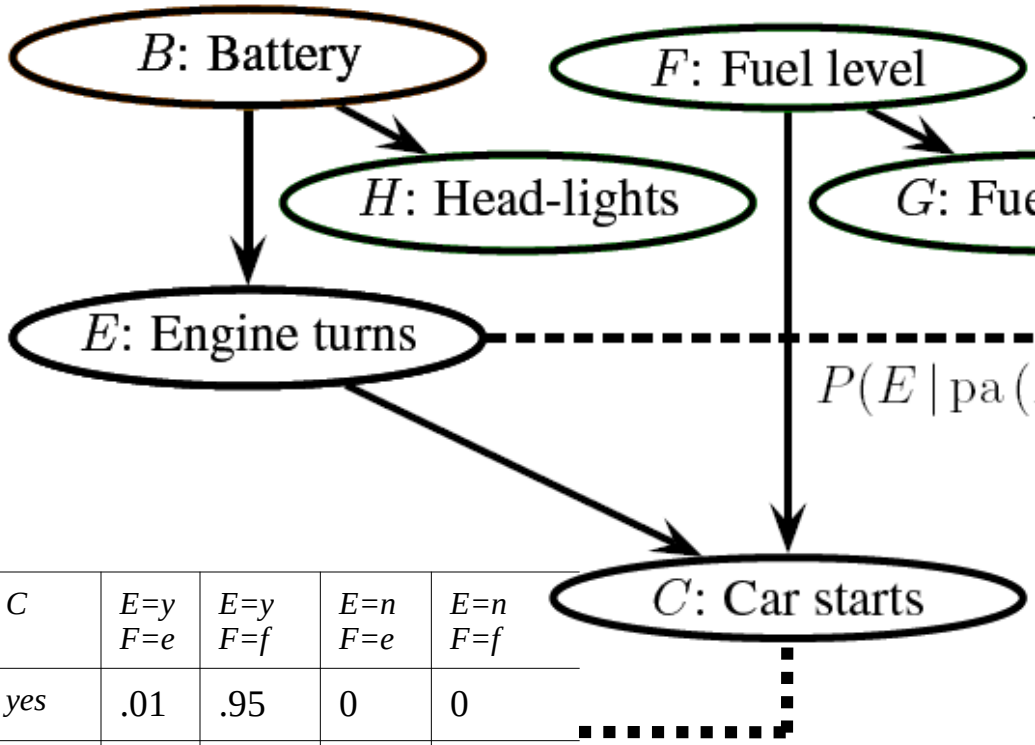
Bayesian Networks

- Bayesian (or Belief) Networks (BN) sono il formalismo piu' usato in IA per rappresentare e ragionare con conoscenza incerta (probabilistica) *[J. Pearl, Probabilistic Reasoning in Inteligence Systems, Morgan Kaufmann, 1988]*
- Sono applicati in una grandissima quantita' di problemi reali
- BN sono definite come un grafo diretto aciclico in cui i nodi sono variabili casuali (discrete), ed ogni variabile ha associata una distribuzione di probabilita' condizionata dalle variabili "genitori" nel grafo (Conditional Probability Table or CPT)

Example: car start (H. Langseth)



$$P(B, F, H, G, E, C)$$



E	B =empty	$B \neq$empty
yes	.01	.97
no	.99	.03

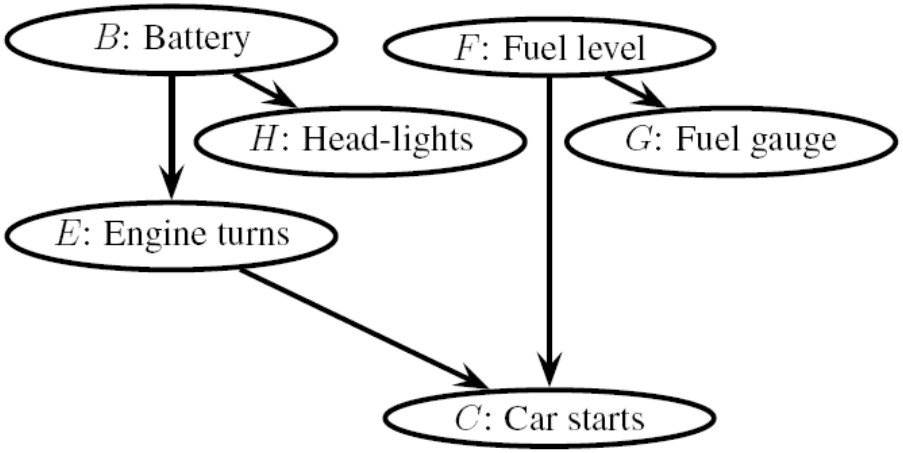
$P(E \mid \mathrm{pa}(E))$

C	*E=y F=e*	*E=y F=f*	*E=n F=e*	*E=n F=f*
yes	.01	.95	0	0
no	.99	.05	1	1

$$P(B,F,H,G,E,C) = P(B)P(F)P(H \mid B)P(G \mid F) \cdot P(E \mid B)P(C \mid E,F)$$

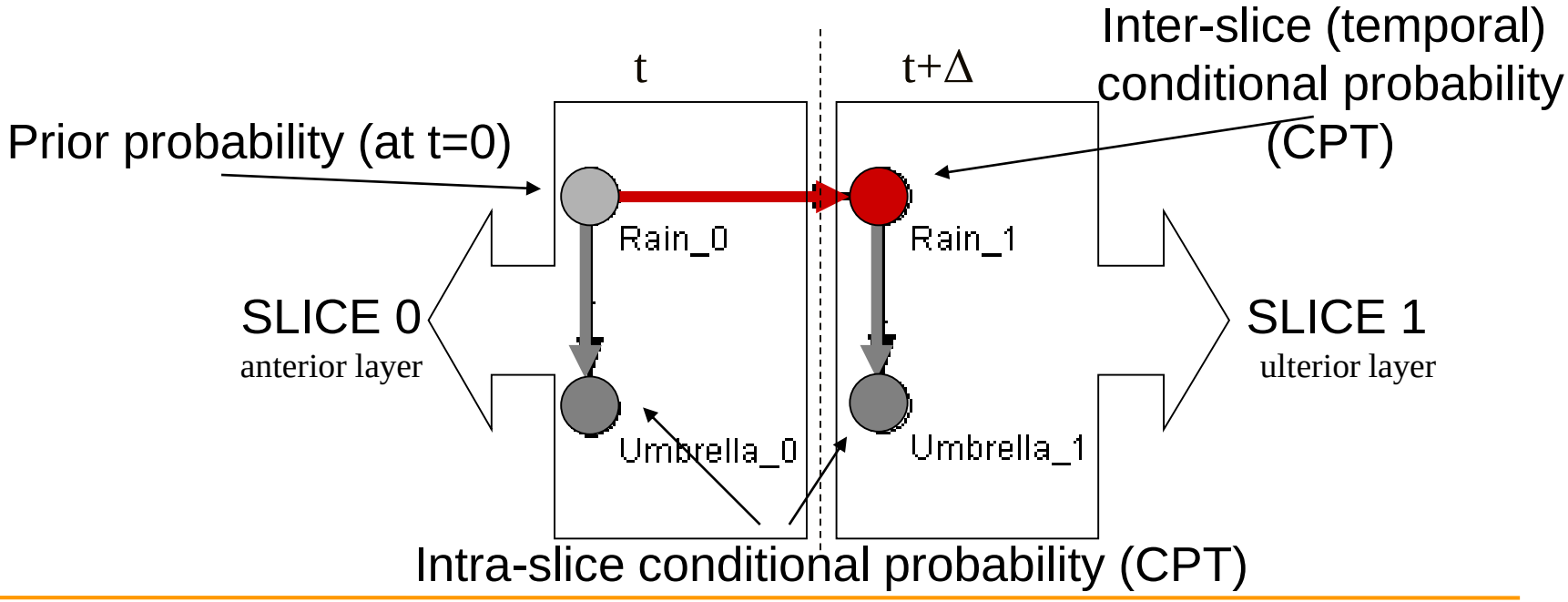
Analisi: computazioni probabilistiche

- Diagnostic inference
  - Pr(cause | effect)
    - Pr(B | C)
    - Pr(F| G)
- Predictive inference
  - Pr(effect | cause)
    - Pr(C | B)
    - Pr(C | F)
- Combined Inference
  - Pr(intermediate|cause, effect)
    - Pr(E | B, C)
- Algoritmi esatti (*Clustering*, *Conditioning*, *Variable Elimination*) o approssimati (*Stochastic Simulation*)

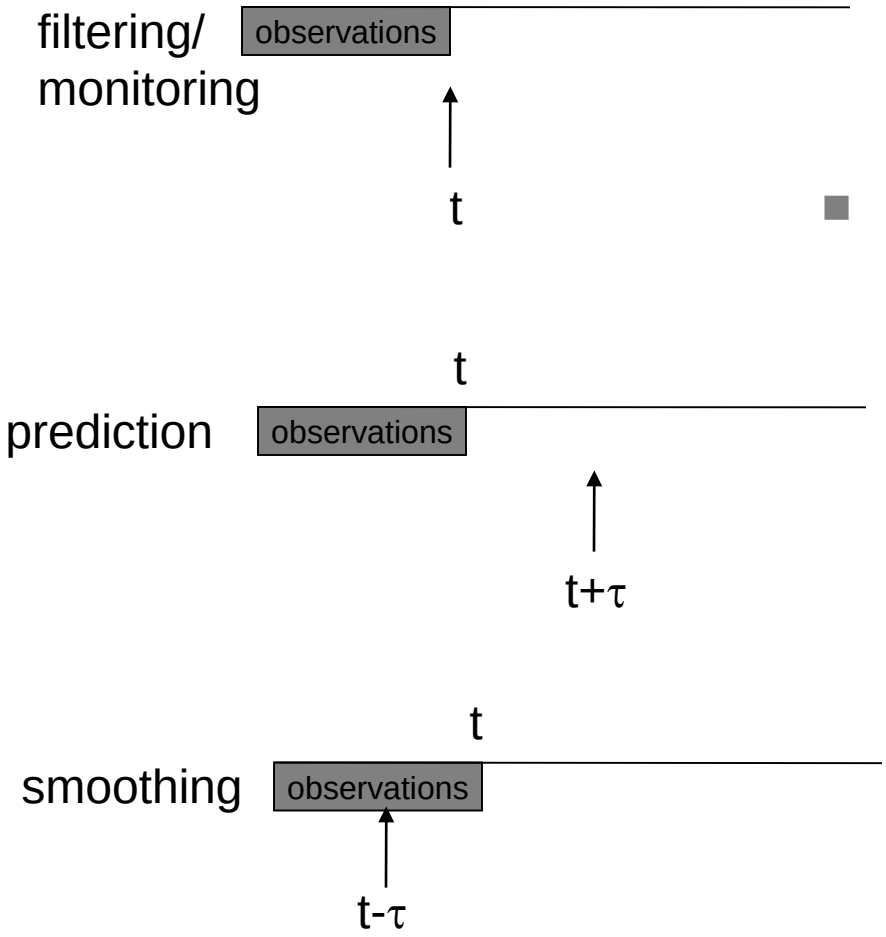


Dynamic Bayesian Networks

- DBN introducono una dimensione temporale **discreta**
  - Il sistema e' rappresentanto a diversi istanti temporali
  - Le dipendenze condizionali tra variabili a tempi diversi catturano l'evoluzione temporale
  - Si assumono tipicamente le proprieta' di Time invariance e di processo markoviano: 2 time slices (t, t+Δ) sono sufficienti (2TBN)



Inference in DBN

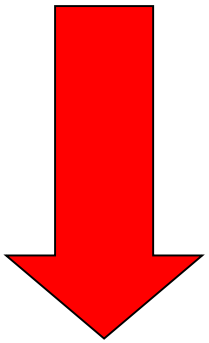


- Algoritmi
  - 1.5 Junction tree (Murphy 02)
  - BK approximation (Boyen-Koller 98)
  - Particle filtering simulation

Sommario

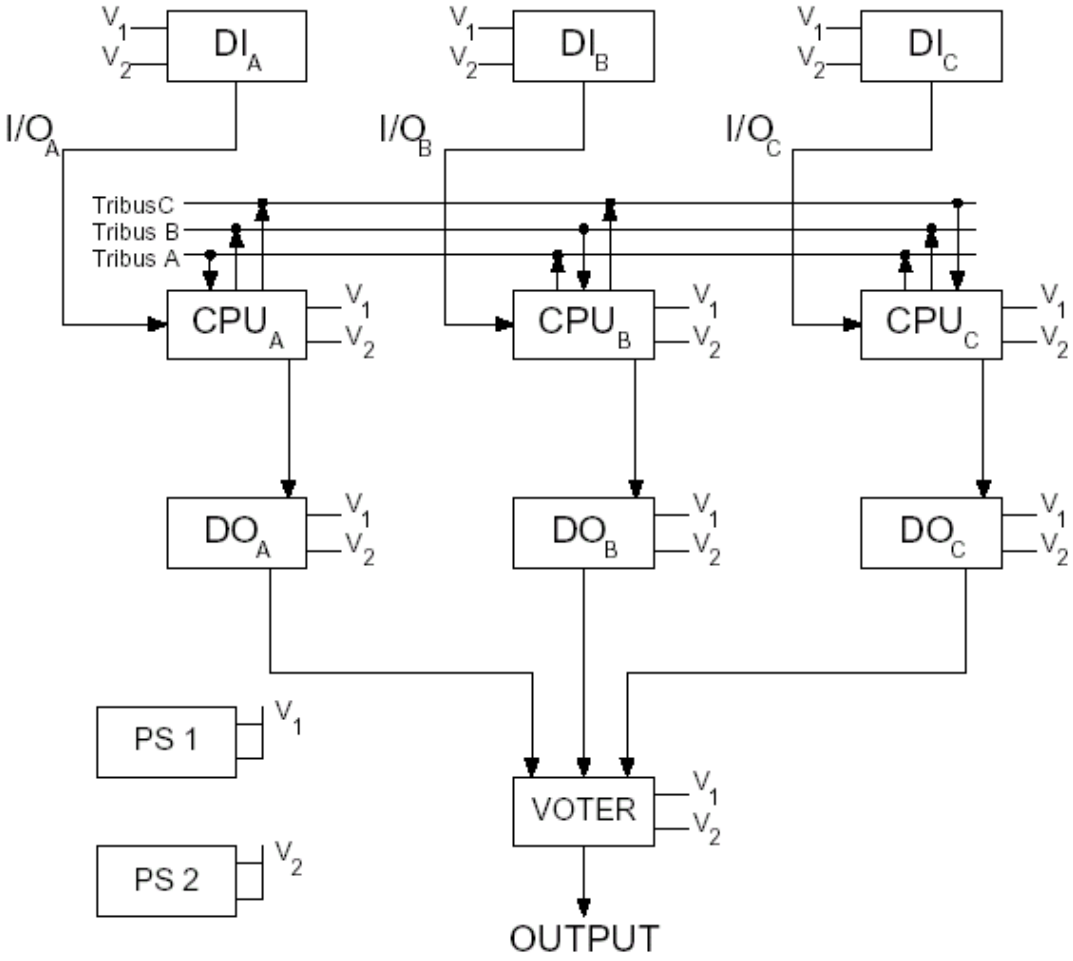
- Dependability, Reliability e FDIR
- Probabilistic Graphical Models (BN and DBN)
  - Reti Bayesiane (Bayesian Networks)
  - Reti Bayesiane Dinamiche (Dynamic Bayesian Networks)
- Dalla Fault Tree Analysis ai modelli grafico-probabilistici
- Case Studies
  - 3ASI Benchmark
  - Cascading failures in a power grid
  - Autonomous FDIR in a mars rover
- Tools
- Open Issues

Possibilita’ di compilare automaticamente un FT in una BN

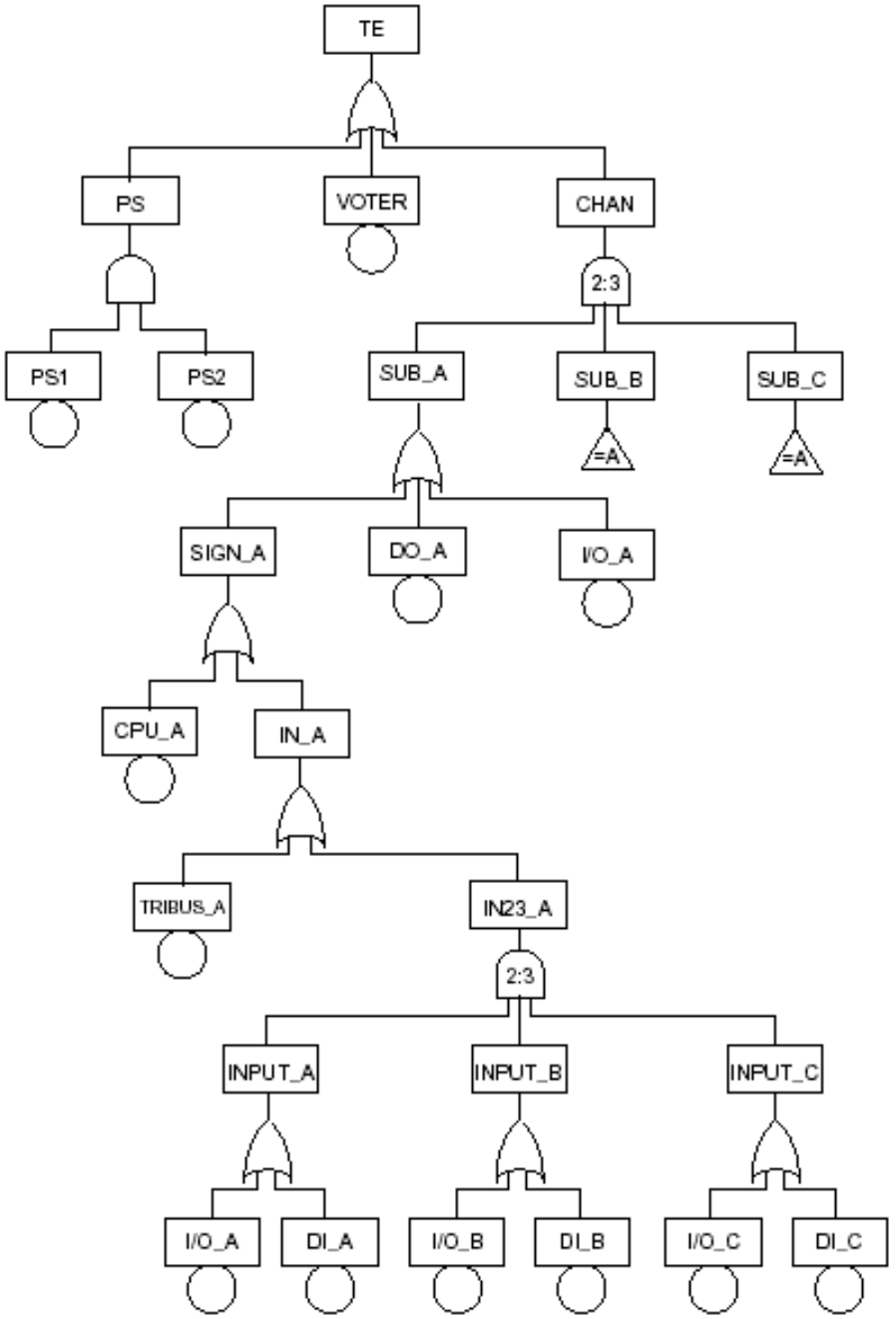


- Aumento di capacita’ di modellizzazione ed analisi
- Capacita’ praticamente completa di FDIR

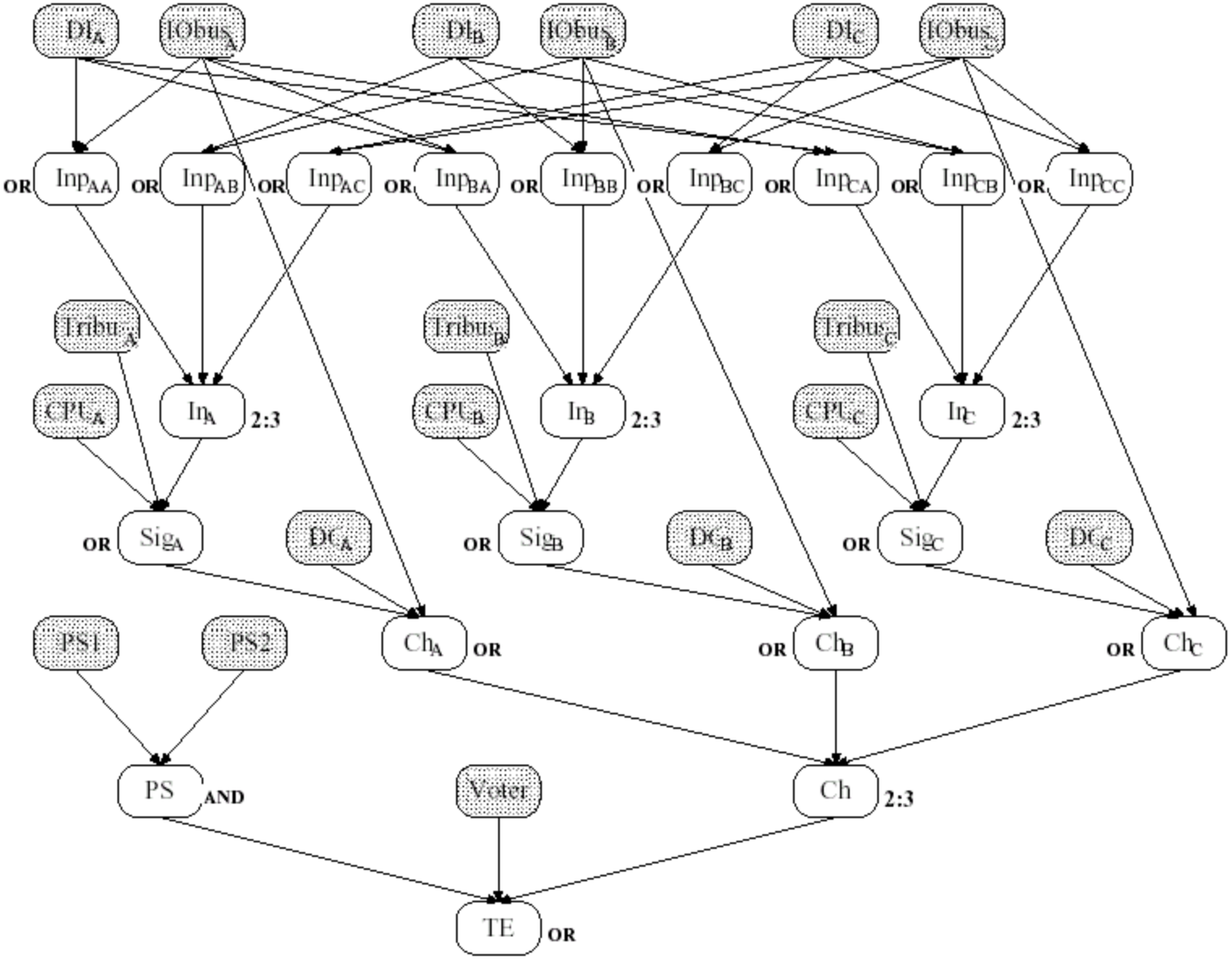
Example: a PLC architecture



PLC: the FT


TE
PS
VOTER
CHAN
2:3
PS1
PS2
SUB_A
SUB_B
SUB_C
=A
=A
SIGN_A
DO_A
I/O_A
CPU_A
IN_A
TRIBUS_A
IN23_A
2:3
INPUT_A
INPUT_B
INPUT_C
I/O_A
DI_A
I/O_B
DI_B
I/O_C
DI_C

PLC: the BN

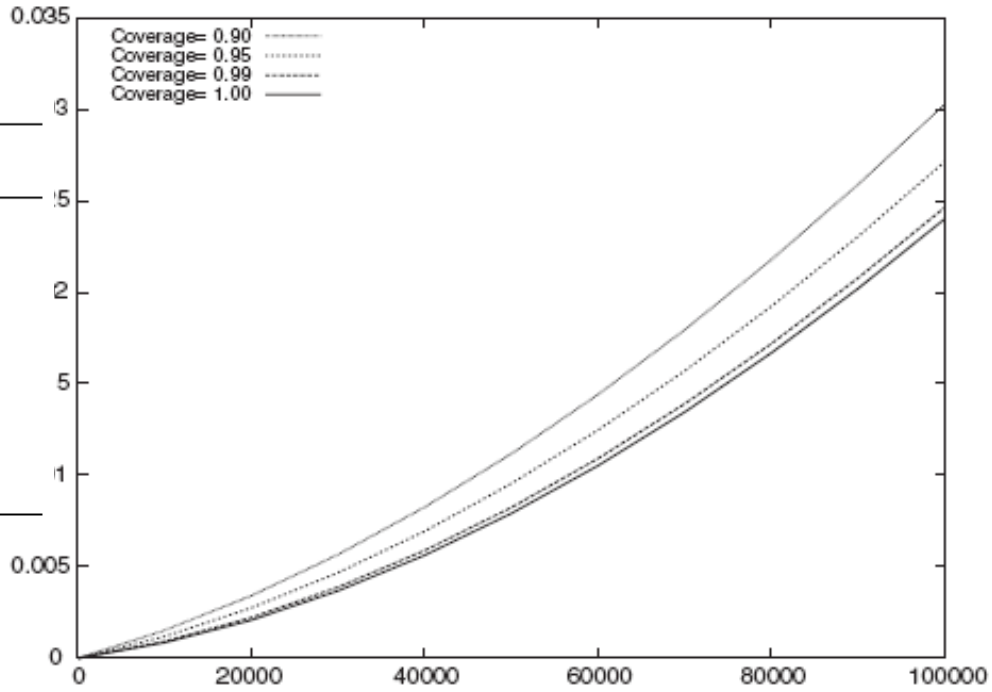

DI_A
IObus_A
DI_B
IObus_B
DI_C
IObus_C
OR
Inp_AA
OR
Inp_AB
OR
Inp_AC
OR
Inp_BA
OR
Inp_BB
OR
Inp_BC
OR
Inp_CA
OR
Inp_CB
OR
Inp_CC
Tribus_A
Tribus_B
Tribus_C
CPU_A
In_A
2:3
CPU_B
In_B
2:3
CPU_C
In_C
2:3
OR
Sig_A
DC_A
OR
Sig_B
DC_B
OR
Sig_C
DC_C
PS1
PS2
Ch_A
OR
OR
Ch_B
OR
Ch_C
PS
AND
Voter
Ch
2:3
TE
OR

Analysis Tasks

- Probability of TE at time t (system's unreliability)
  - Query: *P(TE)* using the probability of basic events (i.e. BN roots) computed at time t (e.g. $P(C=true)=1-e^{-\lambda t}$)

Failure rates (per hour)

Component	Failure rate (h^{-1})
IObus	$\lambda_{IO} = 2.0 \times 10^{-9}$
Tribus	$\lambda_{Tri} = 2.0 \times 10^{-9}$
Voter	$\lambda_{V} = 6.6 \times 10^{-8}$
DO	$\lambda_{DO} = 2.45 \times 10^{-7}$
DI	$\lambda_{DI} = 2.8 \times 10^{-7}$
PS	$\lambda_{PS} = 3.37 \times 10^{-7}$
CPU	$\lambda_{CPU} = 4.82 \times 10^{-7}$



Analysis Tasks

- Posterior probability of each component *C* given the system failure (Fussell-Vesely importance) at time *t*
  - Query: *P(C | TE)* by using priors on roots at time *t*

$$t = 4 \times 10^5 \text{ h}$$

Vesely/Fussell's importance measure

Component	Posterior failure prob.
CPU	0.383
DO	0.204
PS	0.176
DI	0.172
Voter	0.118
IObus	0.002
Tribus	0.002

Analysis Tasks

- Posterior probability of a set of components given the system failure at time *t*
  - Query $P(C_1, \ldots C_n \mid TE)$ at time *t*

$t = 4 \times 10^5$ h

Most probable posterior configurations

Components	Posterior probability
$\{CPU_A, CPU_B\}$	0.045
$\{CPU_B, CPU_C\}$	0.045
$\{CPU_A, CPU_C\}$	0.045
{Voter}	0.027
$\{CPU_A, DO_C\}$	0.022
$\{CPU_A, DO_B\}$	0.022
$\{CPU_B, DO_A\}$	0.022
$\{CPU_B, DO_C\}$	0.022
$\{CPU_C, DO_A\}$	0.022
$\{CPU_C, DO_B\}$	0.022
$\{PS_1, PS_2\}$	0.021

Advanced Modeling Features

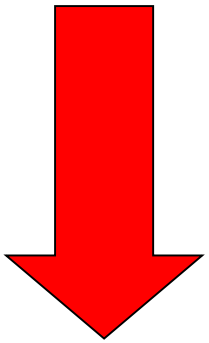
BN aumenta il modeling power wrt FT

- Probabilistic Gates
- Multi-state Variables
- Sequentially Dependent Faults
- Parameter Uncertainty

Sommario

- Dependability, Reliability e FDIR
- Probabilistic Graphical Models (BN and DBN)
  - Reti Bayesiane (Bayesian Networks)
  - Reti Bayesiane Dinamiche (Dynamic Bayesian Networks)
- Dalla Fault Tree Analysis ai modelli grafico-probabilistici
- Case Studies
  - 3ASI Benchmark
  - Cascading failures in a power grid
  - Autonomous FDIR in a mars rover
- Tools
- Open Issues

Possibilita’ di compilare automaticamente un DFT in una DBN



- Aumento di capacita’ di modellizzazione ed analisi
- Capacita’ praticamente completa di FDIR

Il tutto tenendo conto esplicitamente della dinamica del sistema

Sommario

- Dependability, Reliability e FDIR
- Probabilistic Graphical Models (BN and DBN)
  - Reti Bayesiane (Bayesian Networks)
  - Reti Bayesiane Dinamiche (Dynamic Bayesian Networks)
- Dalla Fault Tree Analysis ai modelli grafico-probabilistici
- Case Studies
  - 3ASI Benchmark
  - Cascading failures in a power grid
  - Autonomous FDIR in a mars rover
- Tools
- Open Issues

Benchmark di affidabilità dinamica

Cosa si intende per **affidabilità dinamica**?

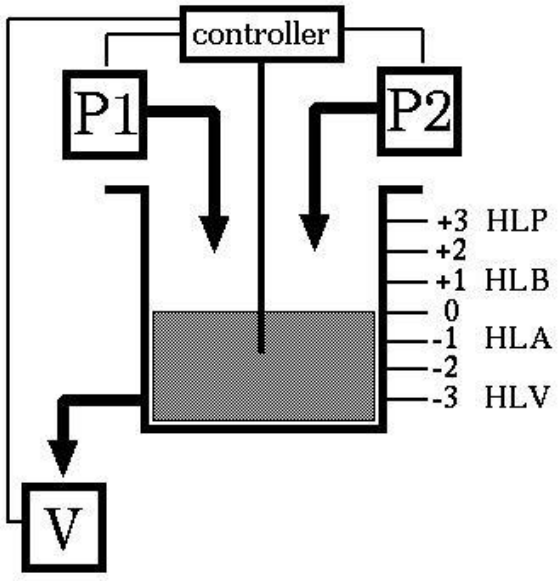
I parametri di affidabilità (tassi di guasto, ecc.) variano a seconda dello stato del sistema e delle azioni svolte.

Il benchmark fu proposto nel 2004 dalla 3ASI (*Analisti dell'Ambiente, dell'Affidabilità e della Sicurezza Industriale*, www.3asi.it). Il benchmark è tratto da

M. Marseguerra, E. Zio, *"Monte Carlo approach to PSA for dynamic process system."* Reliability Engineering and Safety System 52:227-241, 1996

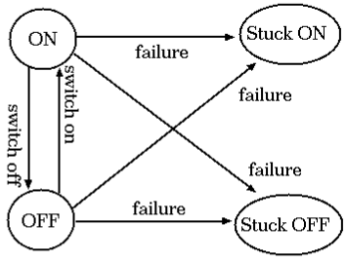
dove è valutato tramite simulazione Monte Carlo

Specifica del benchmark



P1, P2, V: level variation rate: 0.6 m/h.

Failure rates: 0.004566 1/h, 0.005714 1/h, 0.003125 1/h



	Comp. states					Comp. states					Comp. states			
Conf.	P1	P2	V	effect	Conf.	P1	P2	V	effect	Conf.	P1	P2	V	effect
1	OFF	OFF	OFF	=	4	OFF	ON	ON	=	7	ON	ON	OFF	↑↑
2	OFF	OFF	ON	↓	5	ON	OFF	OFF	↑	8	ON	ON	ON	↑
3	OFF	ON	OFF	↑	6	ON	OFF	ON	=					

Control laws:

- $H \leq HLA \Rightarrow$ P1:ON, P2:ON, V:OFF.
- $H \geq HLB \Rightarrow$ P1:OFF, P2:OFF, V:ON.

Failure conditions:

- Dry out (H<HLV)
- Overflow (H>HLP)

Initial configuration:

H = 0

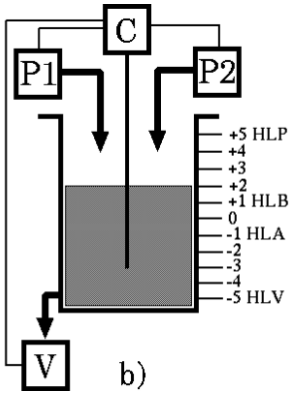
P1 is ON, P2 is OFF, V is ON.

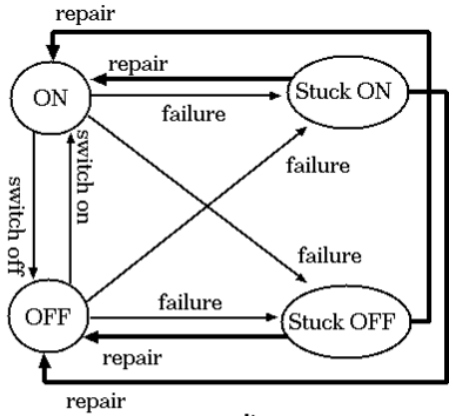
Versioni del benchmark

- **Versione 1**: tassi di guasto costanti
- **Versione 2**: tassi di guasto dipendenti dallo stato del componente (P1, P2, V)

Comp.	State transition from	to	rate
P1	OFF	S_OFF	100λ
P1	OFF	S_ON	10λ
P1	ON	S_ON or S_OFF	λ
P2	OFF	S_ON or S_OFF	λ
P2	ON	S_OFF	100λ
P2	ON	S_ON	10λ
V	OFF	S_OFF	100λ
V	OFF	S_ON	10λ
V	ON	S_ON or S_OFF	λ

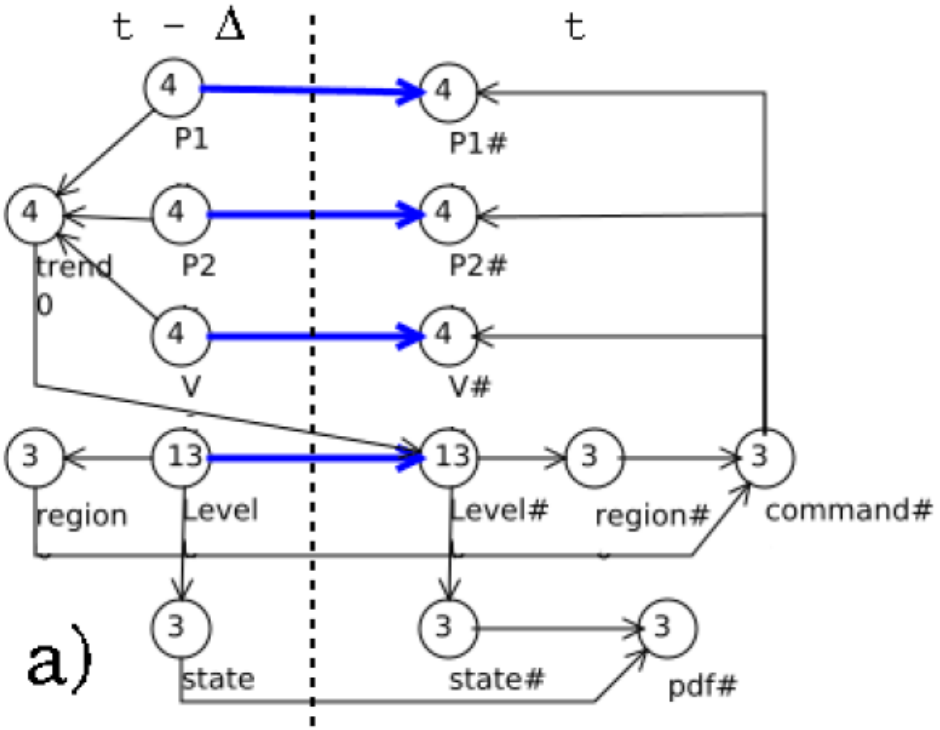
- **Versione 3**: failure on demand (Pr=0.1) del controllore
- **Versione 4**: componenti riparabili



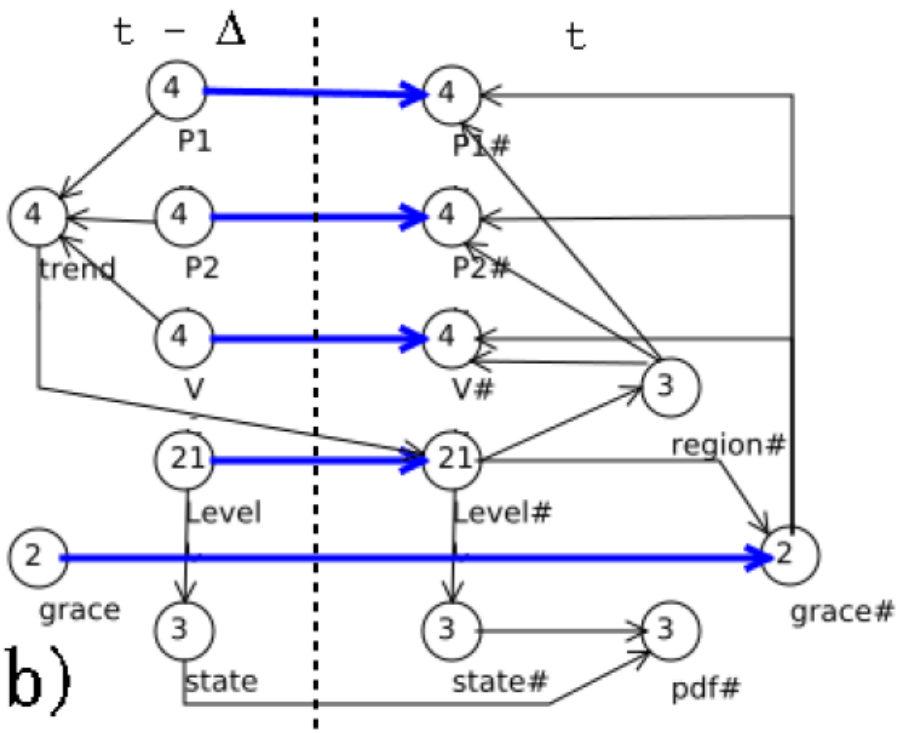


Modelli DBN del benchmark

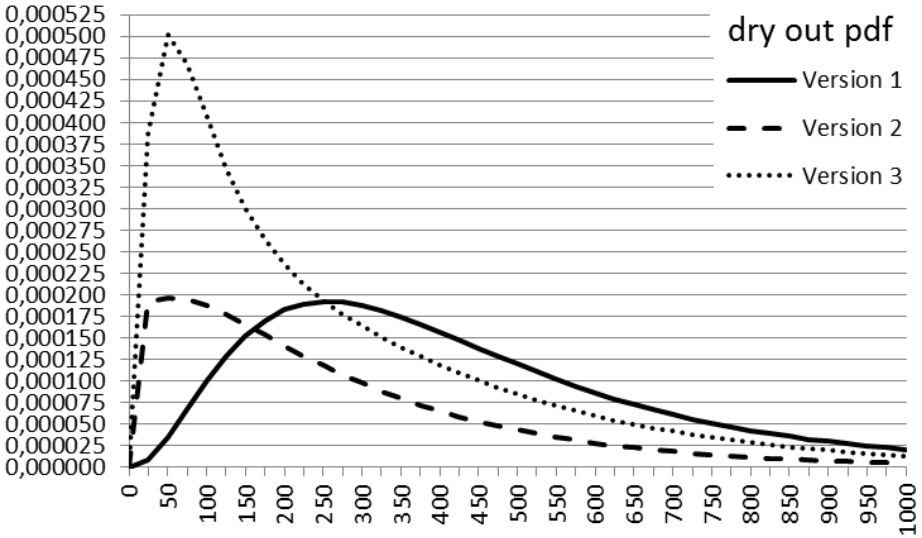
a) Versioni 1, 2, 3

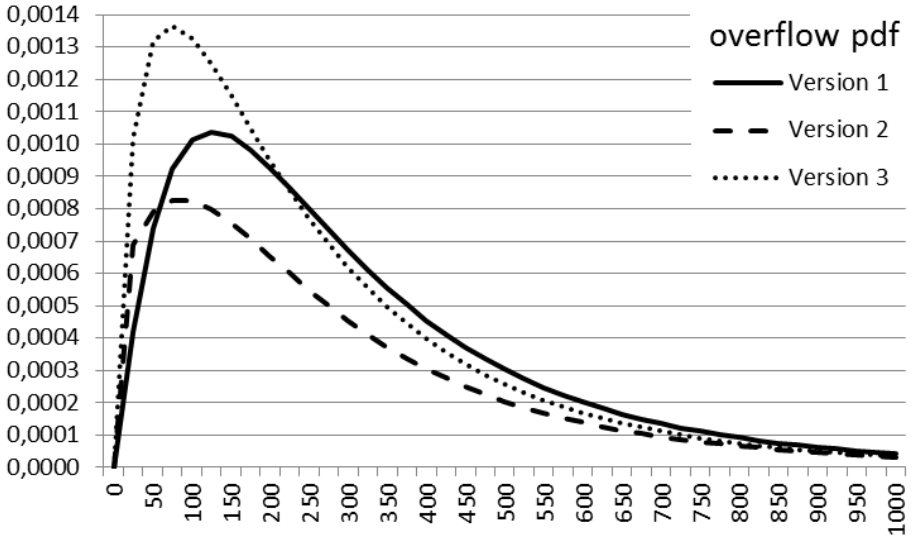


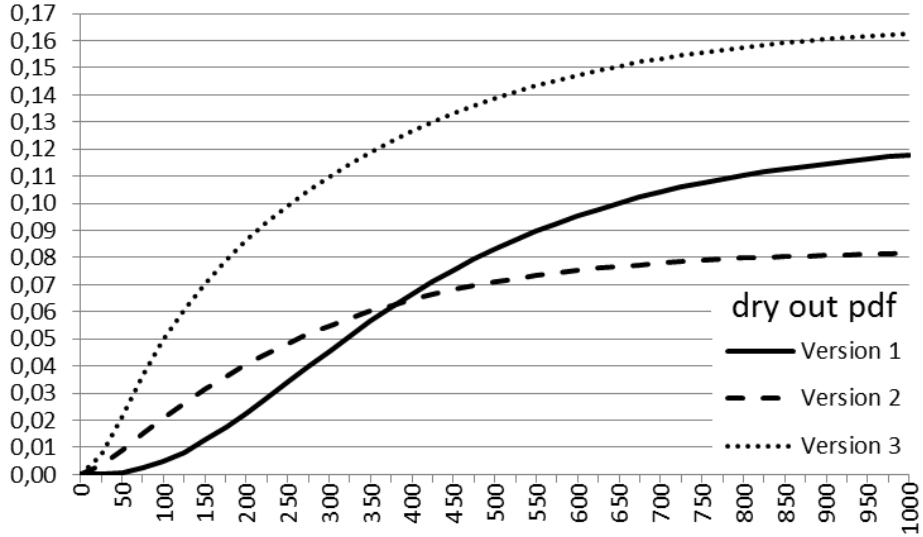
b) Versione 4

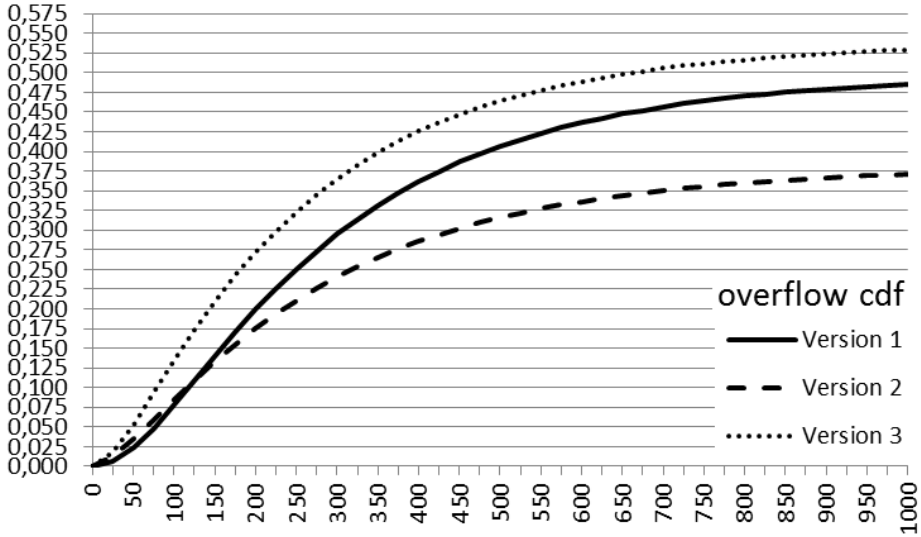


Risultati dell'analisi predittiva (Ver. 1, 2, 3)

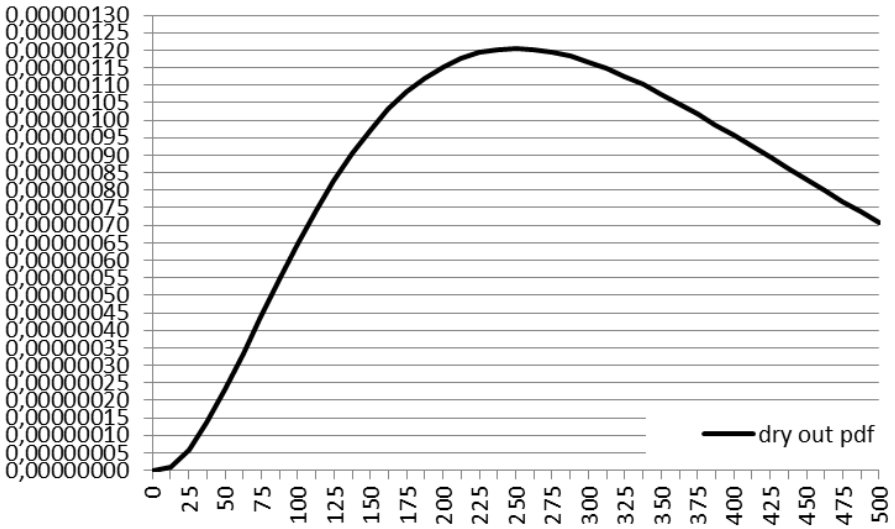


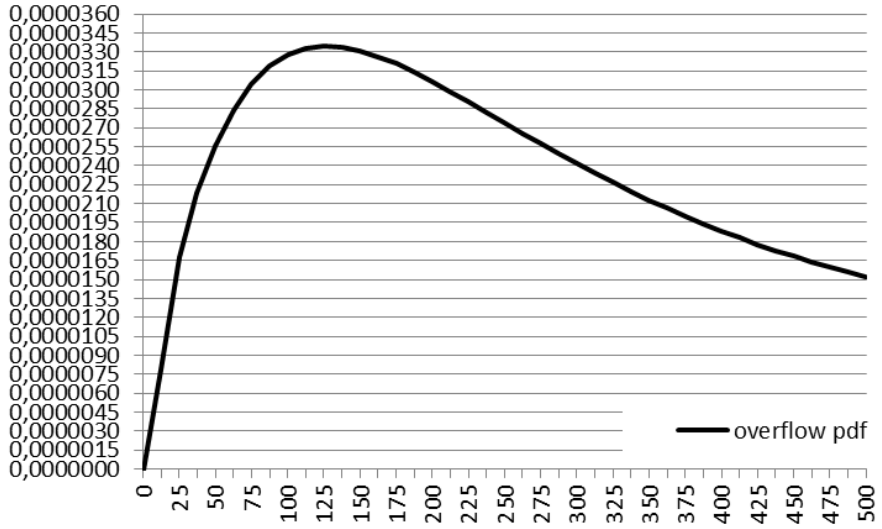


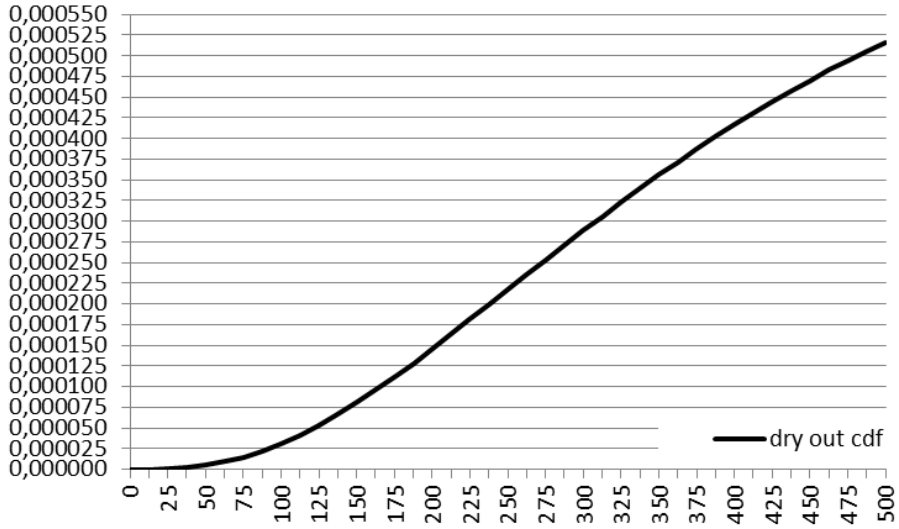


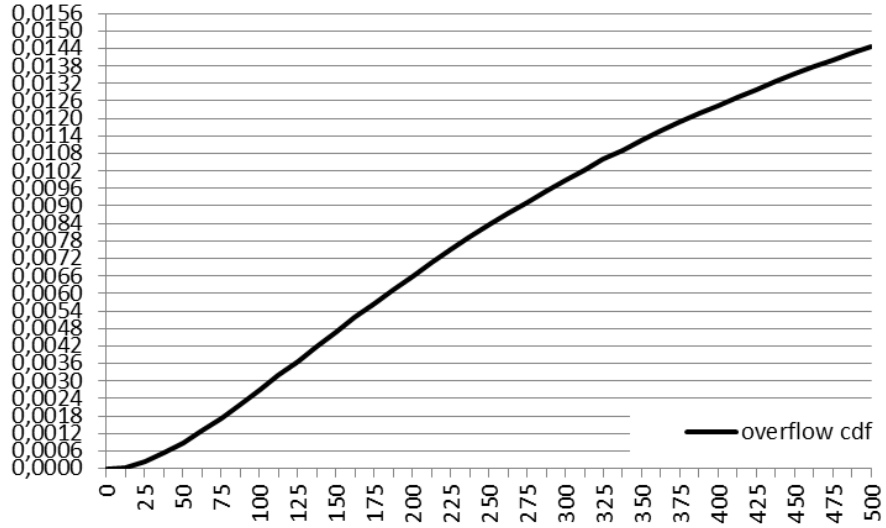


Risultati dell'analisi predittiva (Ver. 4)









Risultati dell'analisi predittiva (confronto)

		dry out				overflow			
time	**steps**	**DBN an.**	SAN sim.	GSPN an.	FSPN sim.	**DBN an.**	SAN sim.	GSPN an.	FSPN sim.
200 h	240	2.2789E-2	2.2390E-2	2.2077E-2	2.400E-2	1.9890E-1	1.9914E-1	1.9518E-1	2.0050E-1
400 h	480	6.6455E-2	6.5990E-2	6.5827E-2	6.730E-2	3.6172E-1	3.6207E-1	3.5987E-1	3.6220E-1
600 h	720	9.5366E-2	9.5290E-2	9.5014E-2	9.360E-2	4.3652E-1	4.3665E-1	4.3568E-1	4.4160E-1
800 h	960	1.1040E-1	1.1003E-1	1.1022E-2	1.084E-1	4.6997E-1	4.7063E-1	4.6959E-1	4.7630E-1
1000 h	1200	1.1777E-1	1.1747E-1	1.1768E-2	1.165E-1	4.8538E-1	4.8572E-1	4.8520E-1	4.9100E-1

Table 14: The cdf values for the dry out and overflow conditions in Version 1.

		Version 2		Version 3		Version 4			
time	**steps**	**DBN an.**	SAN sim.	**DBN an.**	SAN sim.	time	**steps**	**DBN an.**	SAN sim.
200 h	240	4.0657E-2	4.0400E-2	8.6288E-2	8.6710E-2	100 h	120	3.133E-5	6.000E-5
400 h	480	6.4539E-2	6.3360E-2	1.2659E-1	1.2664E-1	200 h	240	1.454E-4	2.200E-4
600 h	720	7.5211E-2	7.3750E-2	1.4738E-1	1.4707E-1	300 h	360	2.882E-4	3.700E-4
800 h	960	7.9762E-2	7.8340E-2	1.5762E-1	1.5739E-1	400 h	480	4.166E-4	4.500E-4
1000 h	1200	8.1656E-2	8.0240E-2	1.6251E-1	1.6220E-1	500 h	600	5.163E-4	5.100E-4

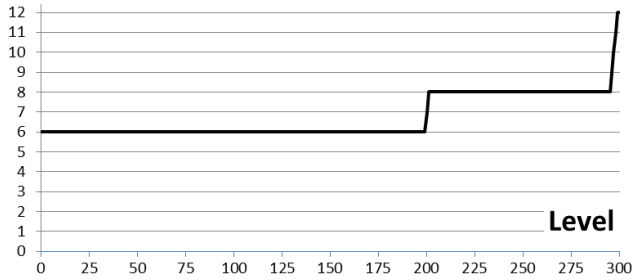
Table 15: The cdf values for the **dry out** condition in Versions 2, 3, 4.

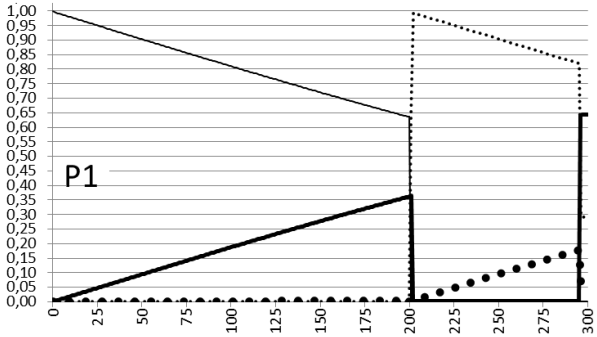
		Version 2		Version 3		Version 4			
time	**steps**	**DBN an.**	SAN sim.	**DBN an.**	SAN sim.	time	**steps**	**DBN an.**	SAN sim.
200 h	240	1.7508E-1	1.6852E-1	2.7222E-1	2.7244E-1	100 h	120	2.686E-3	2.430E-3
400 h	480	2.8591E-1	2.7882E-1	4.2515E-1	4.2492E-1	200 h	240	6.603E-3	6.090E-3
600 h	720	3.3635E-1	3.2938E-1	4.8892E-1	4.8808E-1	300 h	360	9.889E-3	9.460E-3
800 h	960	3.5979E-1	3.5284E-1	5.1649E-1	5.1537E-1	400 h	480	1.245E-2	1.197E-2
1000 h	1200	3.7120E-1	3.6500E-1	5.2900E-1	5.2797E-1	500 h	600	1.447E-2	1.363E-2

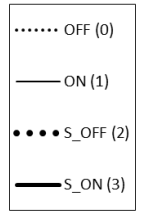
Table 16: The cdf values for the **overflow** condition in Versions 2, 3, 4.

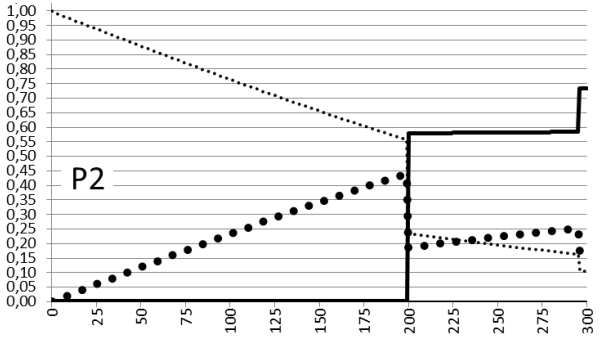
Risultati dell'analisi diagnostica (Scenario 1)

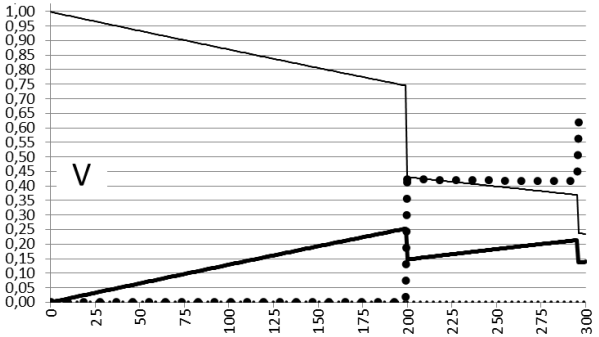
filtering



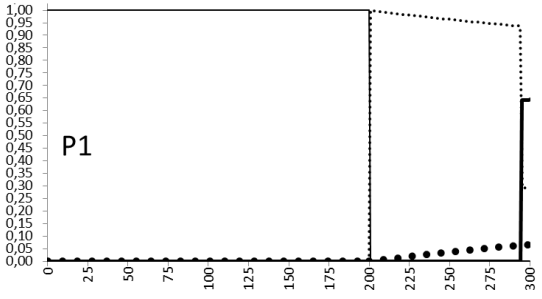


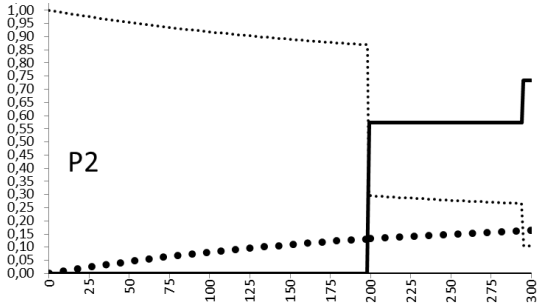


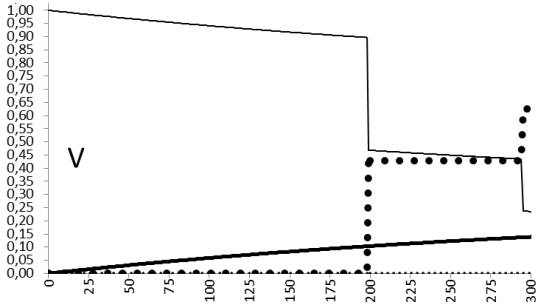




smoothing

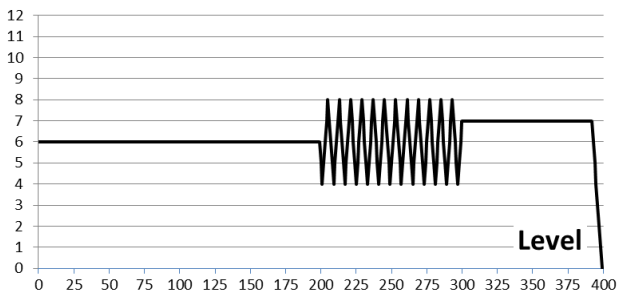


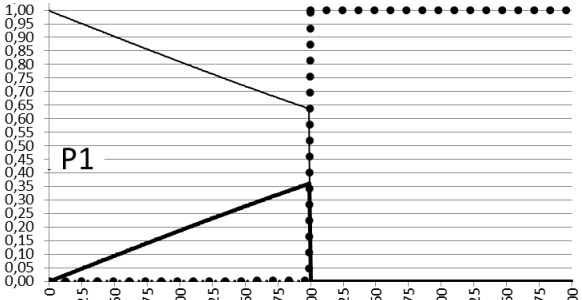


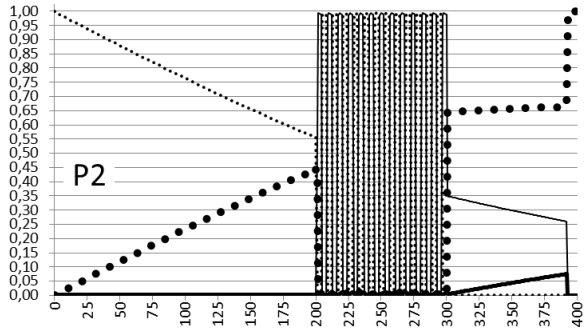


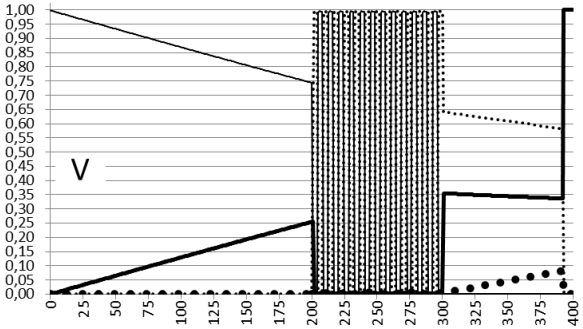
Risultati dell'analisi diagnostica (Scenario 2)

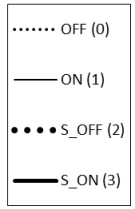
filtering



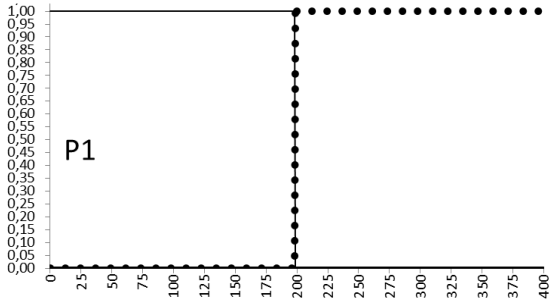


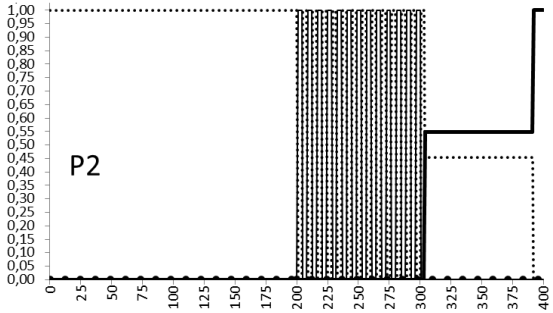


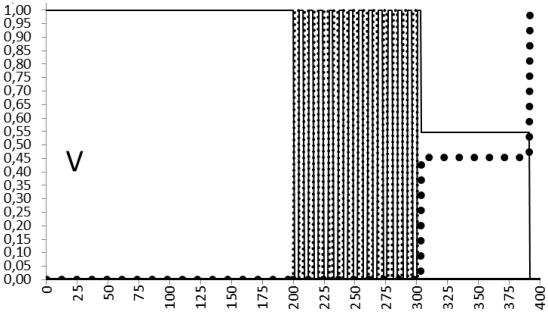




smoothing

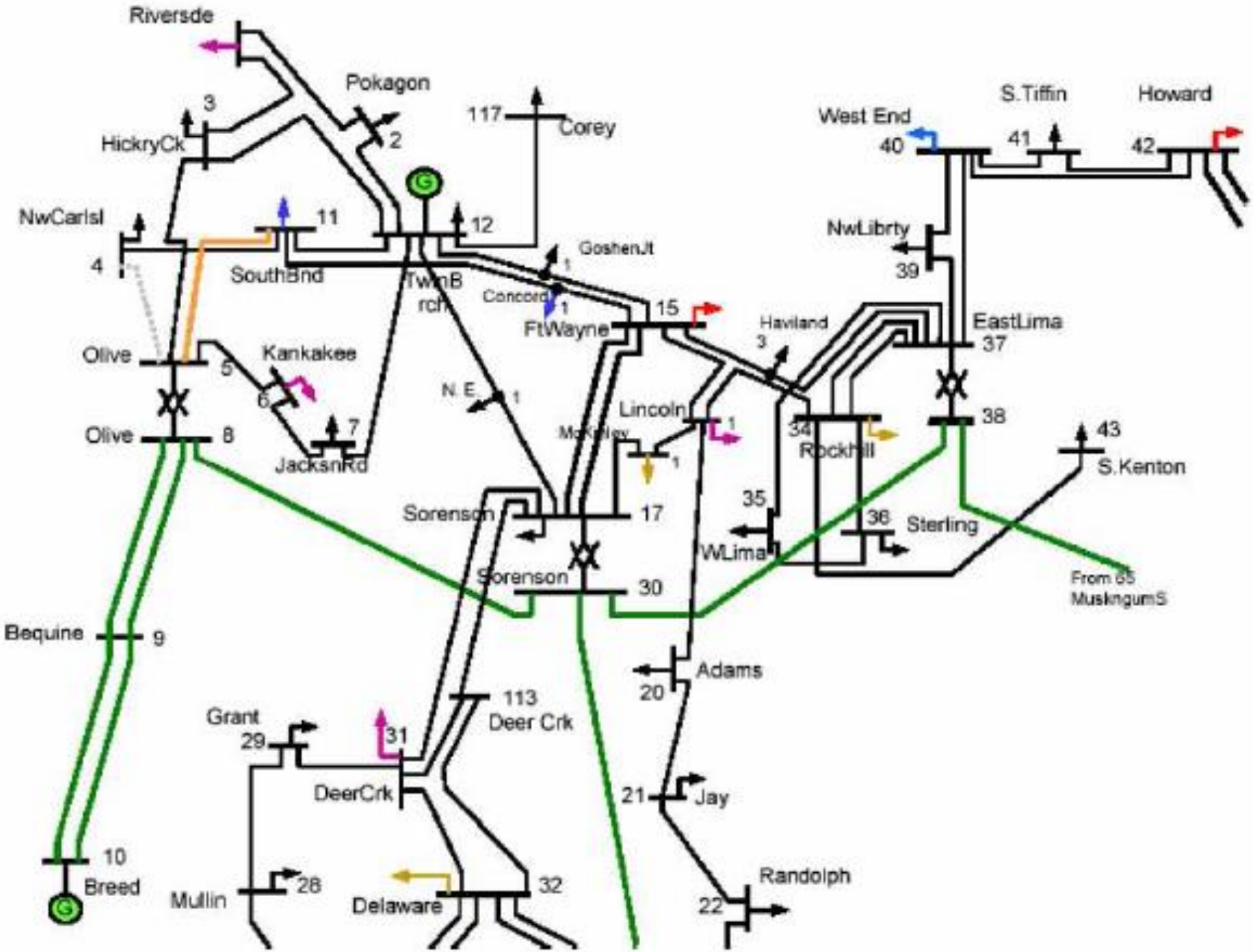




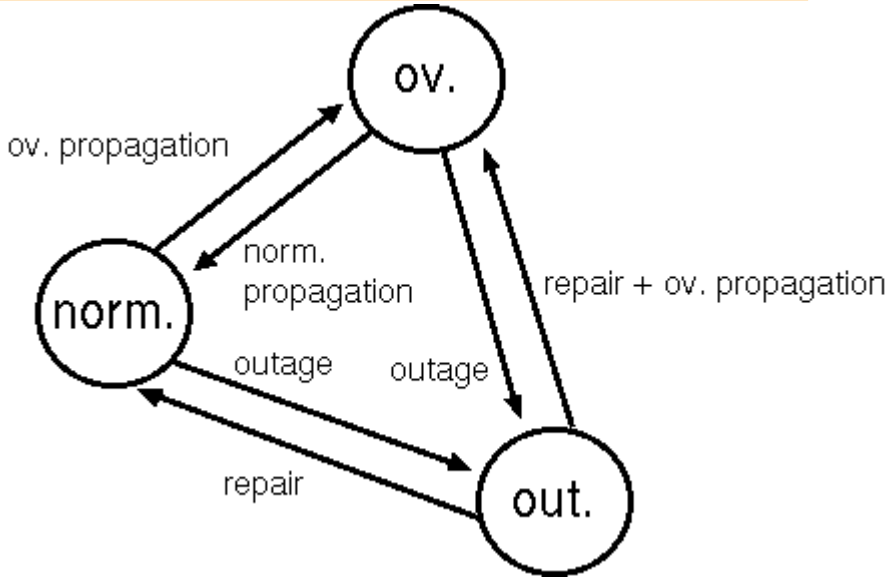


Fallimenti in cascata

- Le interdipendenze tra i componenti di sistemi complessi incrementa il rischio di fallimenti.
- Fallimenti in cascata:
  - Il fallimento di un componente causa un sovraccarico dei componenti adiacenti, aumentando la loro probabilità di fallimento
  - Se non compensato, il sovraccarico/fallimento può causare un progressivo degradamento del sistema. Una parte del sistema potrebbe rimanere isolata dal resto.
    - Per esempio, un blackout in un'area della rete elettrica

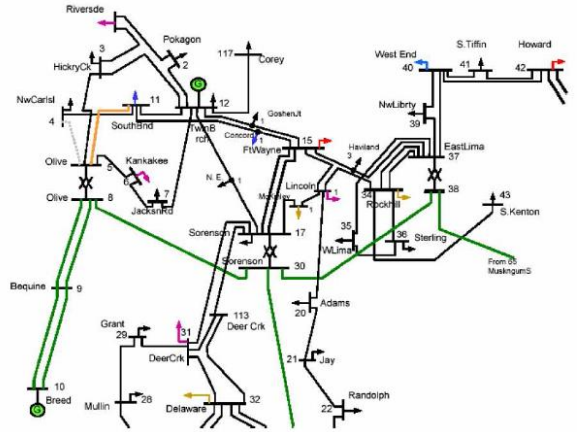

Riversde
Pokagon
3
HickryCk
2
117
Corey
S.Tiffin
Howard
West End
40
41
42
NwCarlsl
11
12
NwLibrty
4
SouthBnd
TwinBrch
GoshenJt
1
Concord
1
39
15
FtWayne
Haviland
3
EastLima
37
Olive
5
Kankakee
6
N. E.
1
Lincoln
1
McKinley
1
34
RockHill
38
43
S.Kenton
Olive
8
7
JacksnRd
35
36
Sterling
Sorenson
17
WLima
Sorenson
30
From 65
MuskingumS
Bequine
9
Adams
20
113
Deer Crk
Grant
29
31
DeerCrk
21
Jay
10
Breed
Mullin
28
Delaware
32
Randolph
22

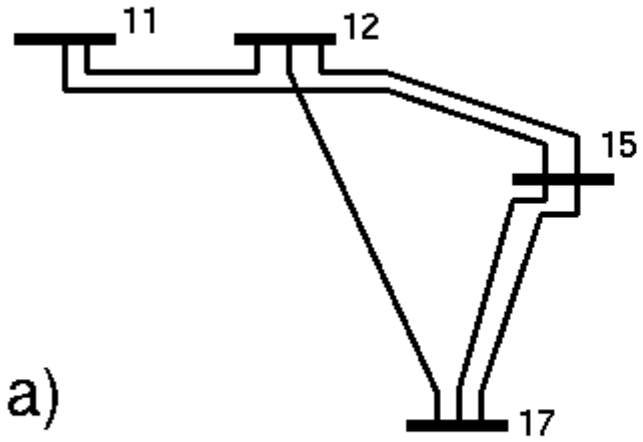
Caratteristiche

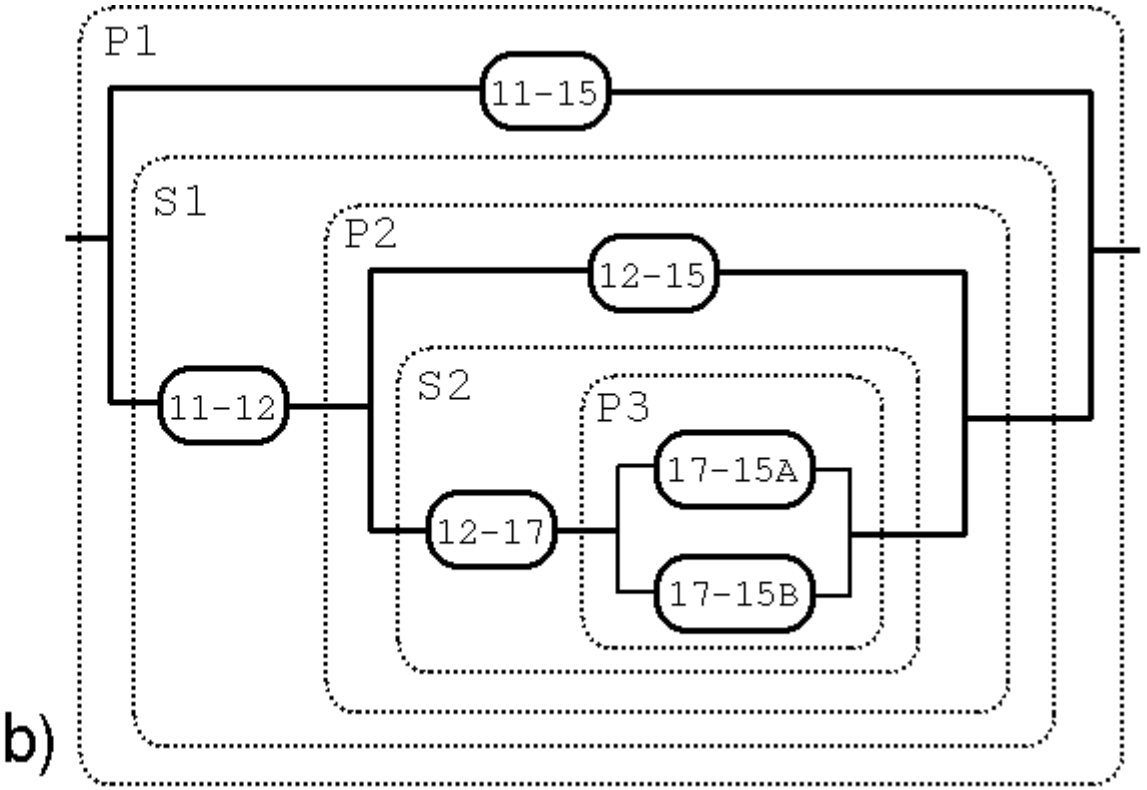


- Stati delle linee
  - normal (carico normale)
  - overloaded (sovraccarica)
  - outaged (guasta)
    - Variabili ternarie nella DBN
  - Guasti e sovraccarichi determinano il sovraccarico di altre linee
- Probabilità di guasto
  - Distribuzione esponenziale negativa
  - Linea funzionante: tasso di guasto $\lambda=0.0001h^{-1}$
  - Linea sovraccarica: tasso di guasto $\alpha\lambda$ ($\alpha=1.2$), $\beta\lambda$ ($\beta=1.5$)

Caso di studio: porzione di rete elettrica



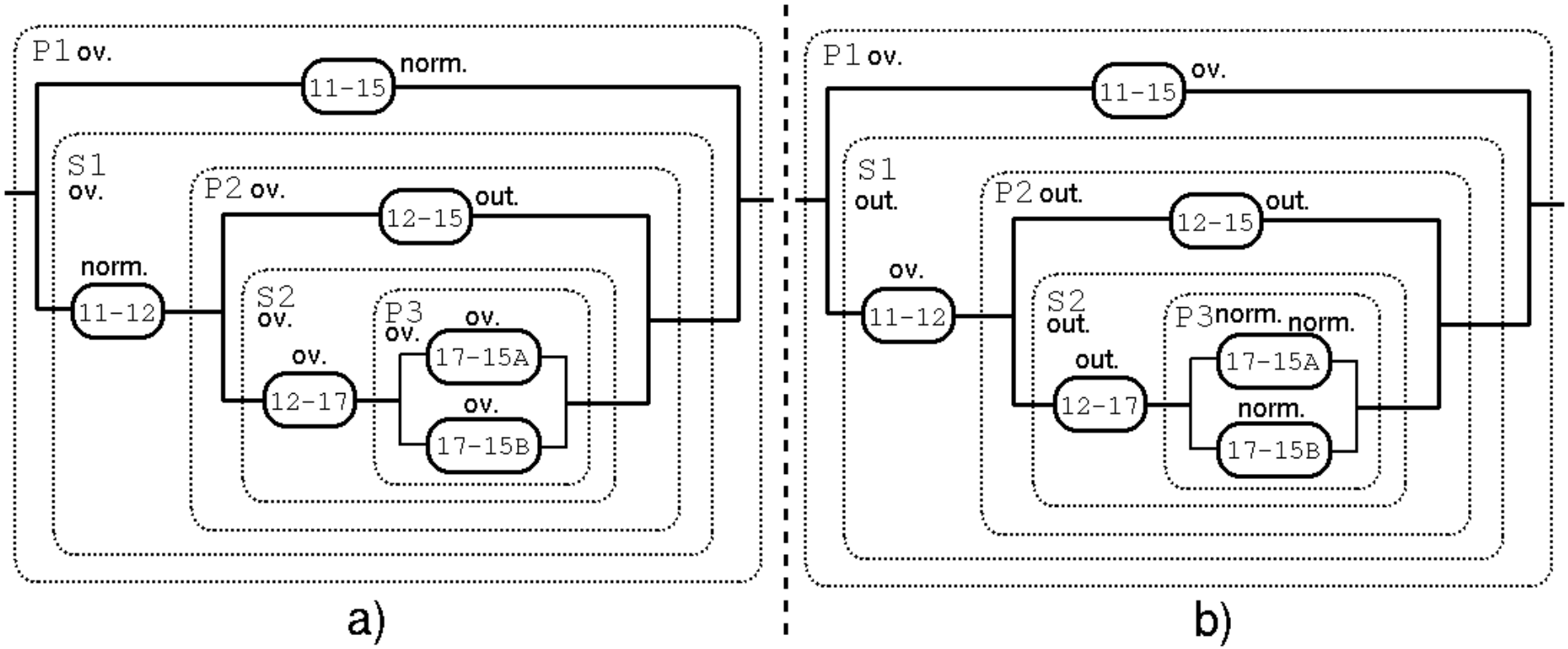




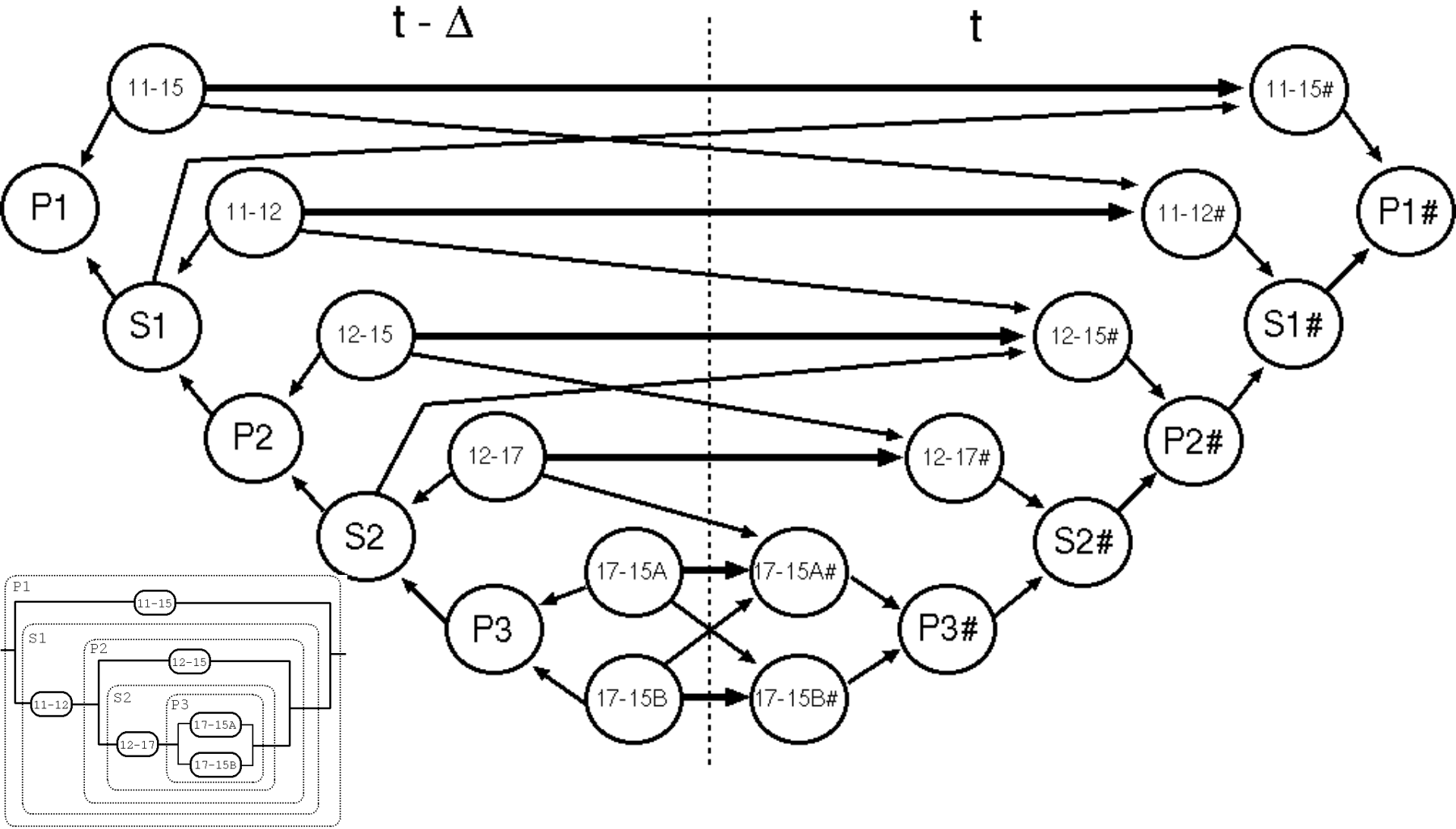
Caso di studio: esempio di scenario

a) Conseguenza del guasto di 12-15

b) Conseguenza del guasto di 12-15 e 12-17



DBN del caso di studio

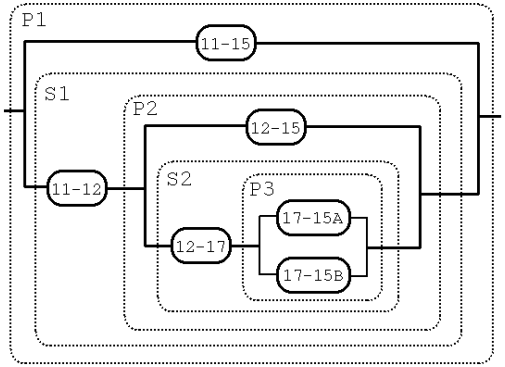


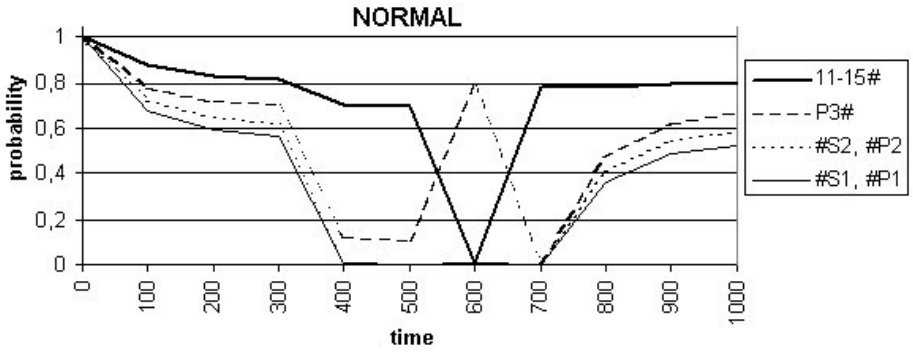
Analisi: filtering

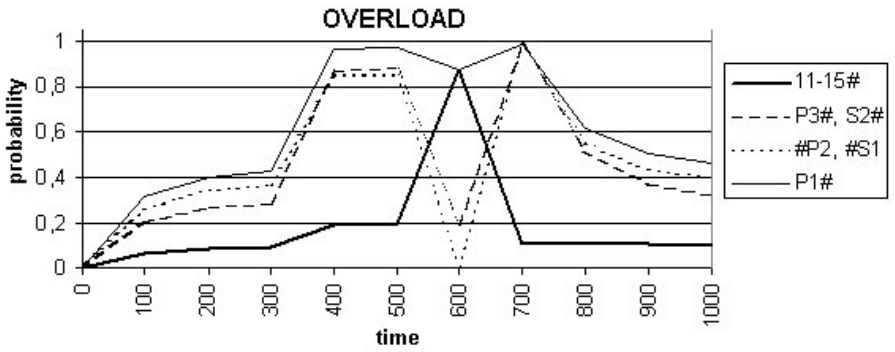
Osservazioni: 12-15 guasta tra i tempi 400h e 700h

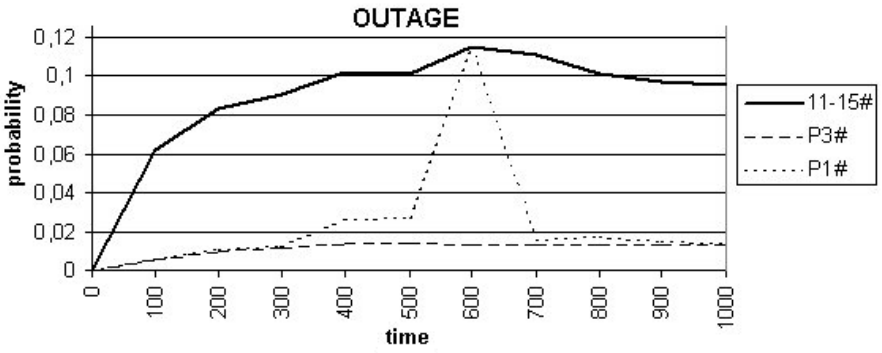
12-17 guasta al tempo 600h

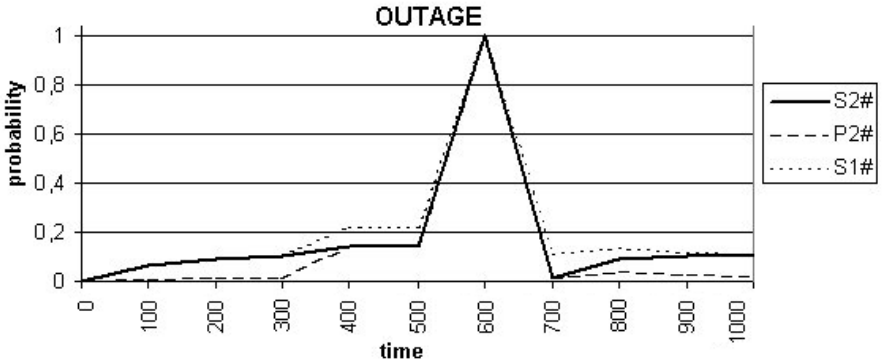
12-17 sovraccarica al tempo 700h









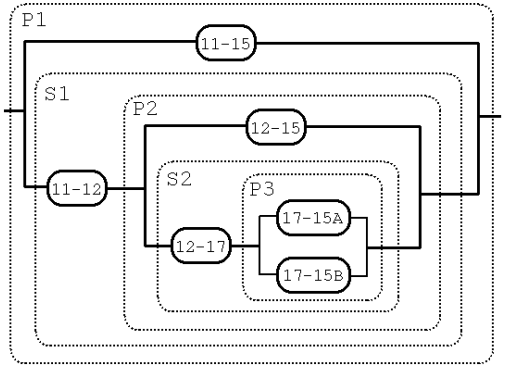


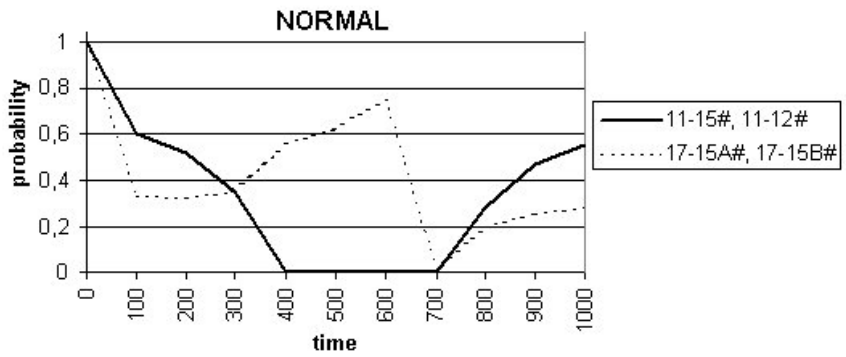
Analisi: smoothing

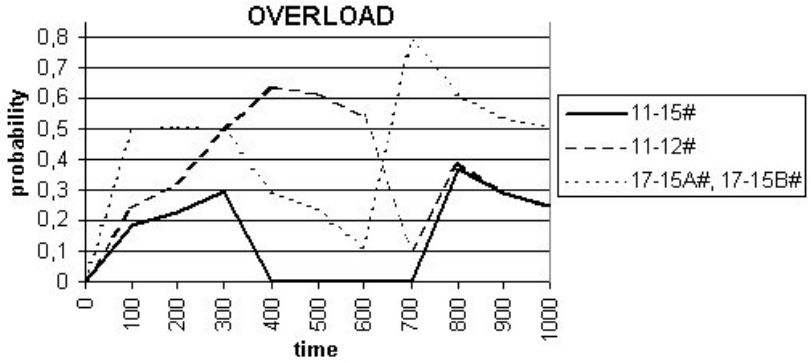
Osservazioni: 12-15 guasta tra i tempi 400h e 700h

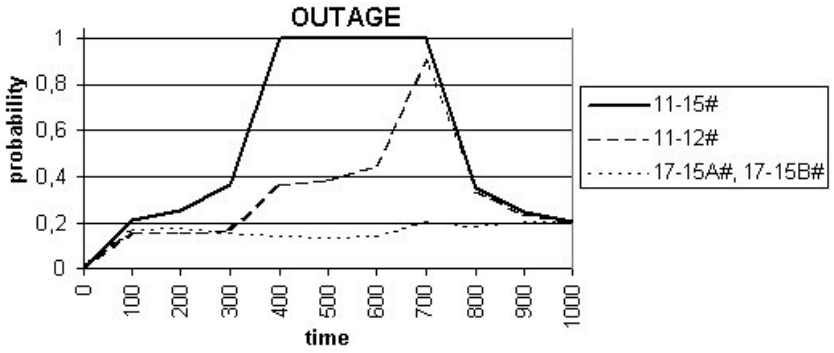
12-17 guasta al tempo 600h

12-17 sovraccarica al tempo 700h





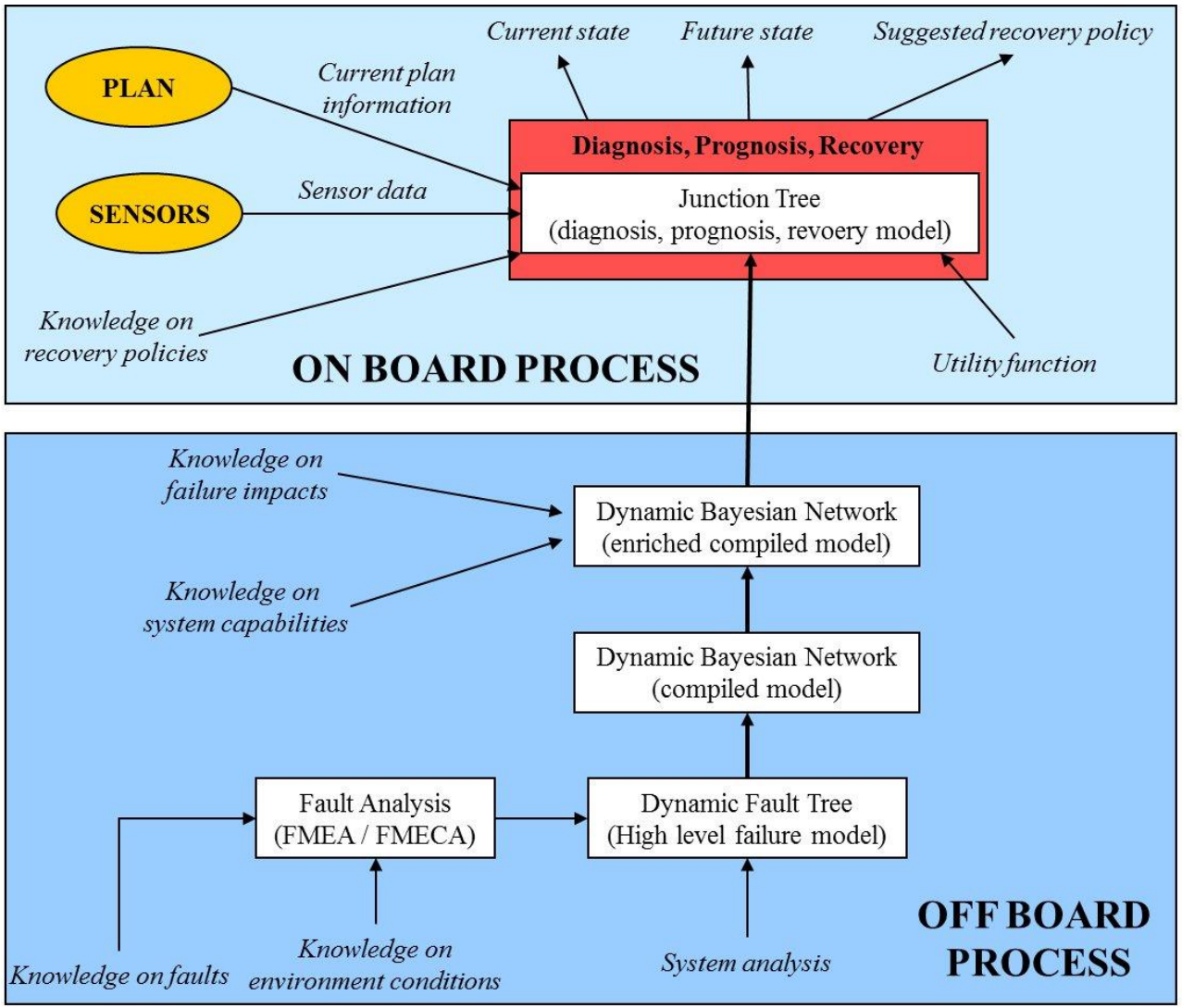




ARPHA: Anomaly Resolution for Prognostic Health management for Autonomy

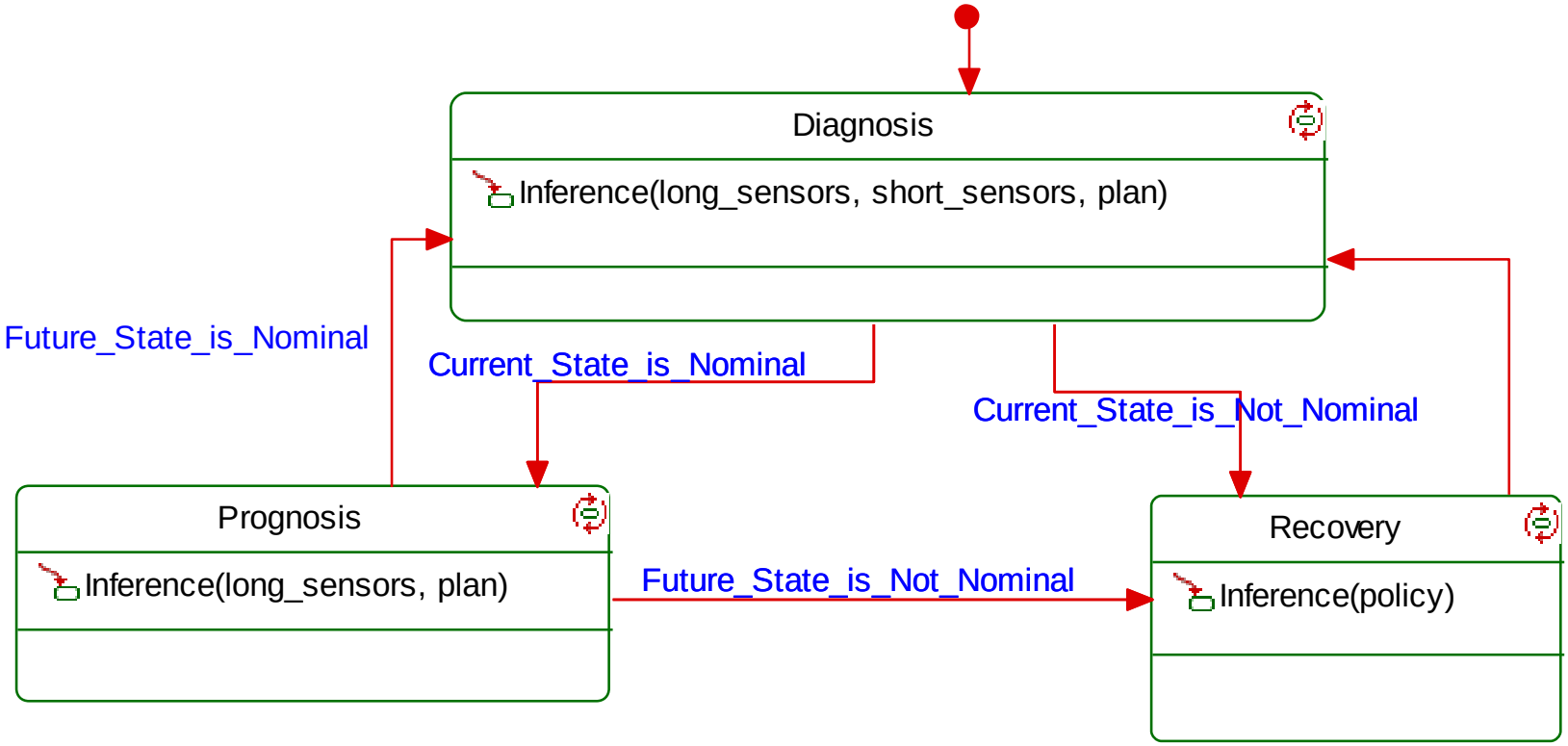
- Software architecture for FDIR analysis based on DBN inference
- Part of the VERIFIM study funded by ESA (partners U.P.O. and Thales/Alenia)
- Case study: Mars Rover power management subsystem reliability

ARPHA Block Scheme

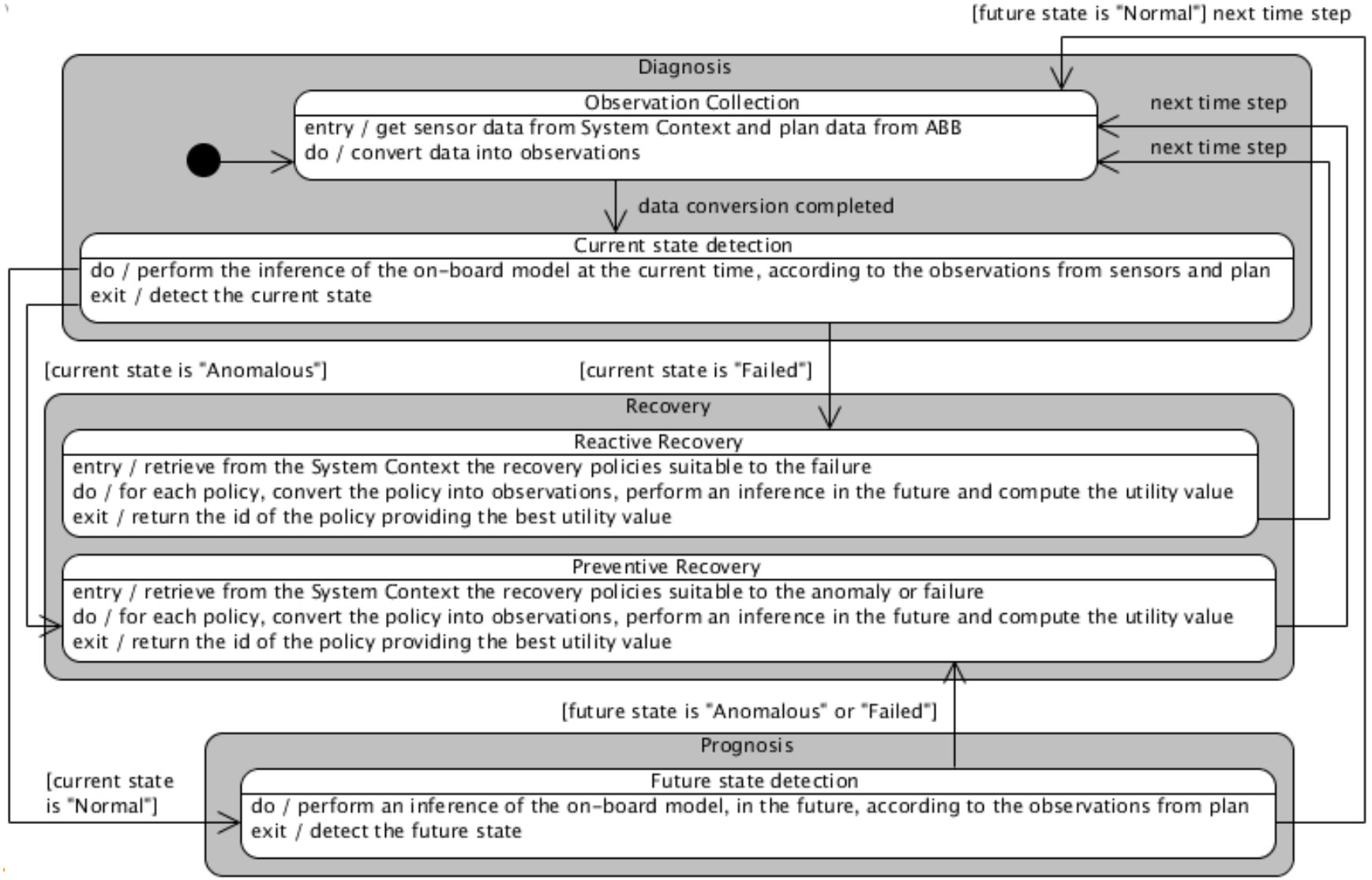


Inference Algorithms: ex-novo ANSI-C (RTEMS) implementation of *1.5JT (Murphy's Algorithm) BK (Boyen-Koller approximation)*

ARPHA on-board process



ARPHA on-board process (in details)

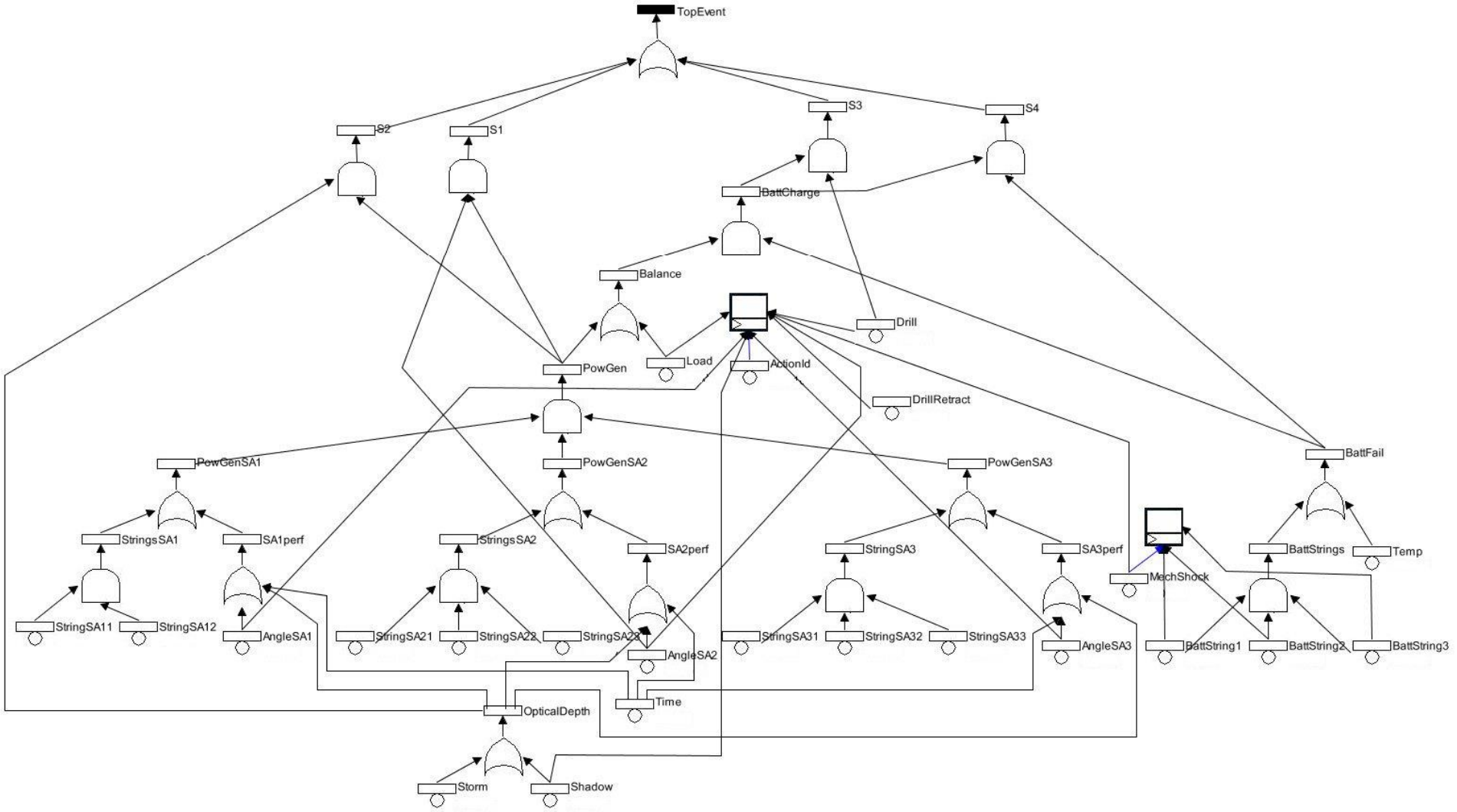


Case study: power supply of a planetary rover

The case study deals with the power supply system of the rover, with a particular attention to the following aspects and their combinations:

- the power supply by the solar arrays: 3 solar arrays, namely SA1, SA2, SA3. Each solar array can generate power if two conditions hold:
  - at least one string is not failed;
  - the combination of sun aspect angle, optical depth, and local time (day or night) is suitable.
- the load: The amount of load depends on the current action performed by the rover
- the power supply by the battery composed by three redundant strings:
  - The charge of the battery may be steady, decreasing or increasing according to the current levels of load and generation by the solar arrays
  - The charge of the battery may be compromized by the damage of the battery occurring in two situations:
    1. all the strings are failed,
    2. or the temperature of the battery is low.
- Scenarios:
  - Slope of terrain (S1): the presence of a terrain slope increases sun aspect angle by causing lower power generation of solar array
  - Presence of dusty (S2) : the presence of dust increases optical depth and reduces power generated by solar arrays.
  - Problem during drilling (S3) : we simulate an unexpected high request of energy by drill.
  - Damage to battery system (S4): we simulate a damage to battery that reduces battery charge level.

Dynamic Fault Tree model



Scenarios and policies (1/2)

We are interested in 4 failure or anomaly scenarios. Each scenario can be recovered by specific policies:

Scenario 1: slope of terrain.

Recovery policies:

P1) suspension of the plan in order to reduce the load

P2) change of inclination of SA2 and SA3 in order to try to improve the sun aspect angle and consequently the power generation (the tilting system can not act on SA1)

Scenario 2: presence of dusty.

Recovery policies:

P3) movement of the rover into another position in order to try to avoid a shadowed area and improve the power generation as a consequence

P4) modication of the inclination of SA2 and SA3, retraction of the drill, and suspension of the plan

Scenarios and policies (2/2)

Scenario 3: problem during drilling.

Recovery policies:

P4) as in scenario 2

P5) retraction of the drill, suspension of the plan

Scenario 4: damage to battery system.

Recovery policies:

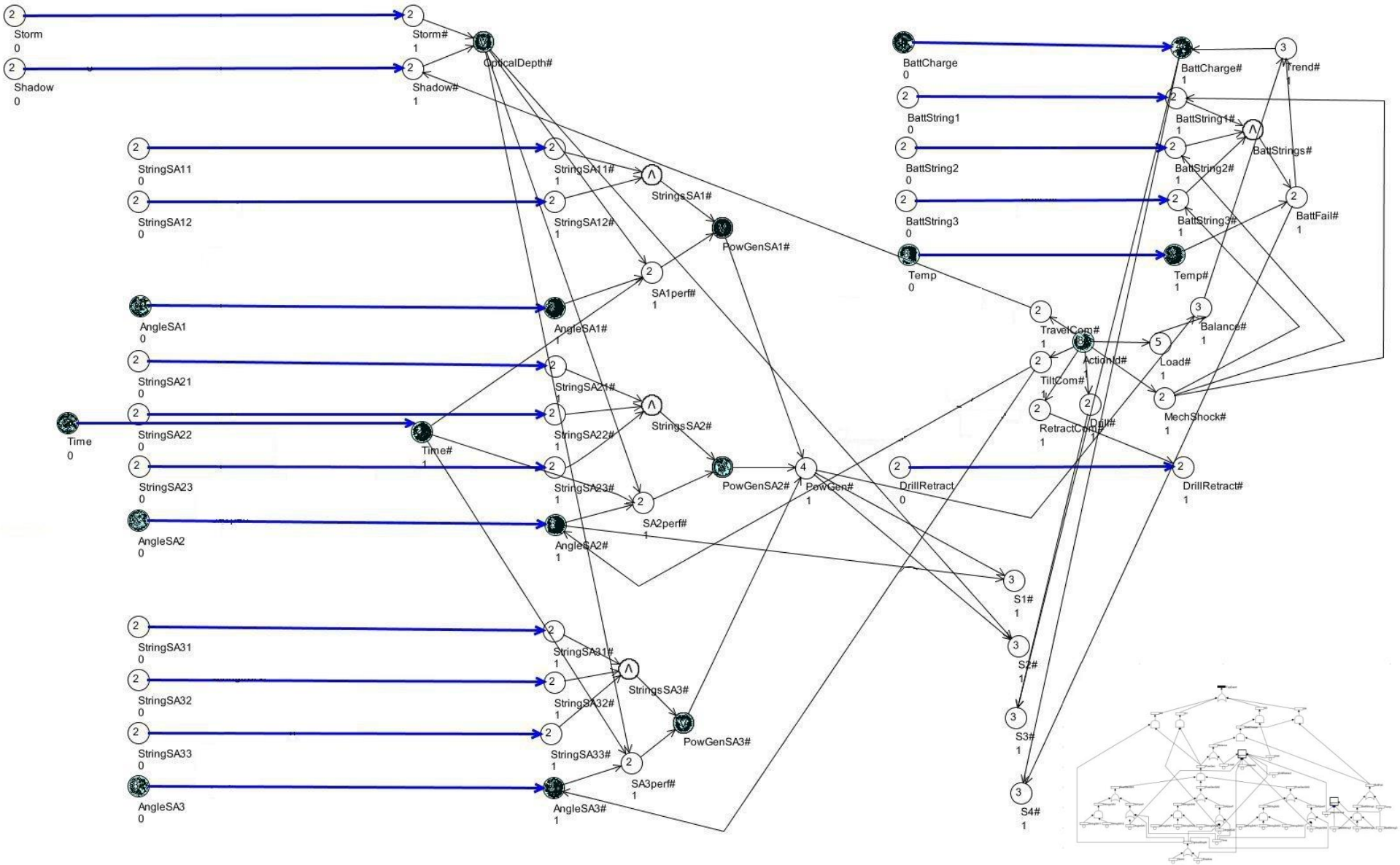
P4) as in scenario 2 and scenario 3

From DFT to DBN

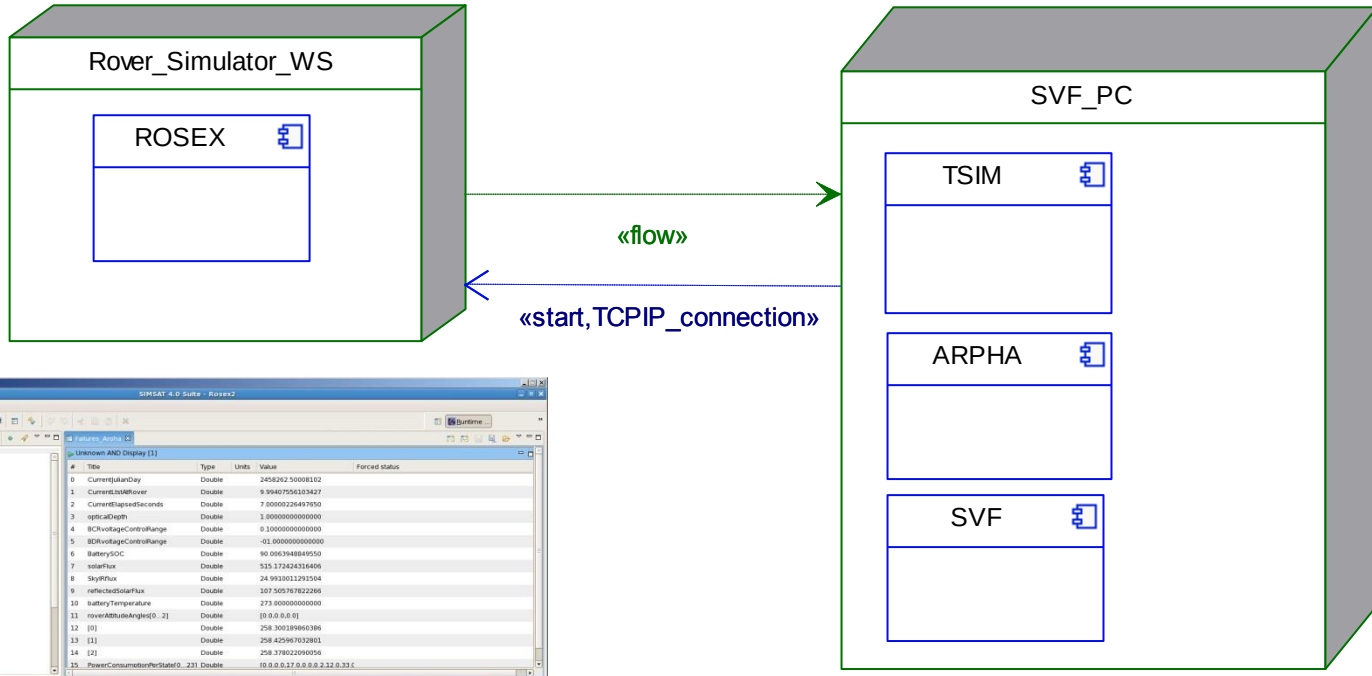
- Conversion of the DFT into DBN
  - DFT events become DBN variables
  - DFT gates determine the CPTs of the DBN variables

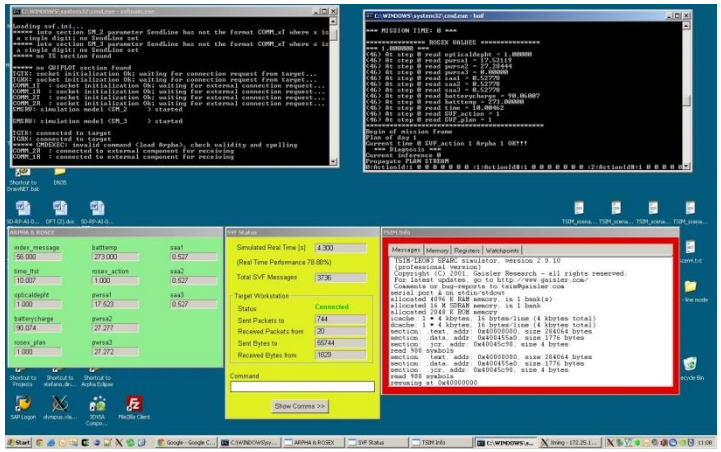
- Enrichment of the resulting DBN
  - Increase of the size of several variables
    - Multi-state components, conditions, events, levels, ...
  - Update of conditional probability tables (CPT)
    - Non binary variables
    - Non Boolean relations among variables
  - Addition of support variables in order to reduce the number of CPT entries
    - «divorcing» technique

Dynamic Bayesian Network

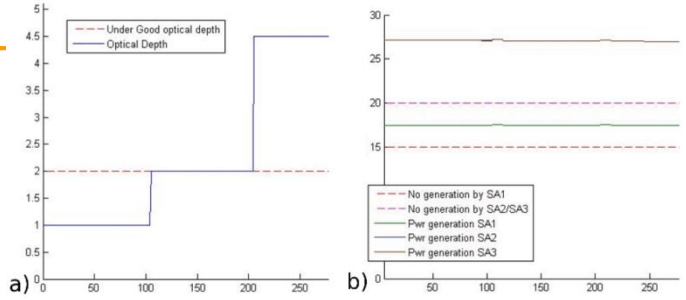


Evaluation Platform





ARPHA output




```
*** MISSION STEP: 3 (MISSION TIME: 218 sec.) ***
*************** ROSEX VALUES ***************
opticaldepht = 4.50000      pwrsa1 = 17.22273       pwrsa2 = 26.67850       pwrsa3 = 26.67641
saa1 = 0.51575              saa2 = 0.51575          saa3 = 0.51575          batterycharge = 90.28925
batttemp = 273.00000        time = 10.05112         SVF_action = 1          SVF_plan = 1
*********************************************
  *** Diagnosis ***
Propagate PLAN STREAM
3:ActionId#:1 0 0 0 0 0 0 0
Propagate SENSORS STREAM
3:OpticalDepth#:0 1 :    3:PowGenSA1#:1 0 :      3:PowGenSA2#:1 0 :        3:PowGenSA3#:1 0 :     3:AngleSA1#:1 0 0 :3:
AngleSA2#:1 0 0 :        3:AngleSA3#:1 0 0 :     3:BattCharge#:0 0 0 1 :   3:Temp#:0 1 0 :        3:Time#:1 0 :
Current inference (STEP 3)
Pr{S1#=2}=0.000<0.990   Pr{S2#=2}=0.000<0.590   Pr{S3#=2}=0.000<0.990   Pr{S4#=2}=0.000<0.990
Pr{S1#=1}=0.000<0.990   Pr{S2#=1}=0.000<0.590   Pr{S3#=1}=0.000<0.990   Pr{S4#=1}=0.000<0.990
SYSTEM STATE: "Normal"
  ## Prognosis ##
Propagate PLAN STREAM
4:ActionId#:1 0 0 0 0 0 0 0 :   5:ActionId#:1 0 0 0 0 0 0 0 :   6:ActionId#:1 0 0 0 0 0 0 0 :   7:ActionId#:0 0 1 0 0 0 0 0 :
Future inference (STEP 7)
Pr{S1#=2}=0.38471501<0.99   Pr{S2#=2}=0.60604805>=0.59   Pr{S3#=2}=0.01966910<0.99   Pr{S4#=2}=0.05214530<0.99
Pr{S1#=1} excluded because under recovery or minor criticality   Pr{S2#=2} excluded because under recovery or minor criticality
Pr{S3#=1}=0.09944675<0.99   Pr{S4#=1}=0.29860398<0.99
FUTURE SYSTEM STATE: "Failed" (S2#=2)
  ## Preventive Recovery ##
Policy to convert: P3
Propagate POLICY STREAM
4:ActionId#:0 0 1 0 0 0 0 0 :      5:ActionId#:0 0 1 0 0 0 0 0 :
Future inference (STEP 13)
Utility Function = 0.0890
Policy to convert: P4
Propagate POLICY STREAM
4:ActionId#:0 0 0 0 0 0 1 0 :   5:ActionId#:0 0 0 0 0 0 1 0 :   6:ActionId#:0 0 0 0 0 0 0 1 :   7:ActionId#:0 0 0 0 0 0 0 1 :
8:ActionId#:1 0 0 0 0 0 0 0 :   9:ActionId#:1 0 0 0 0 0 0 0 :   10:ActionId#:1 0 0 0 0 0 0 0 :  11:ActionId#:1 0 0 0 0 0 0 0 :
12:ActionId#:1 0 0 0 0 0 0 0 :  13:ActionId#:1 0 0 0 0 0 0 0 :
Future inference (STEP 13)
Utility Function= 0.8764
Best policy for Preventive Recovery is P4
```

Overview

- Dependability/Reliability issues
- Main Model Types for Reliability
- Probabilistic Graphical Models (BN and DBN)
  - Modeling
  - Computing
- From (Dynamic) Fault Trees to (Dynamic) Bayesian Nets
  - Modeling
  - Computing
- Case Studies
- Tools
- Open Issues

RADYBAN: Reliability Analysis with DYnamic BAyesian Networks

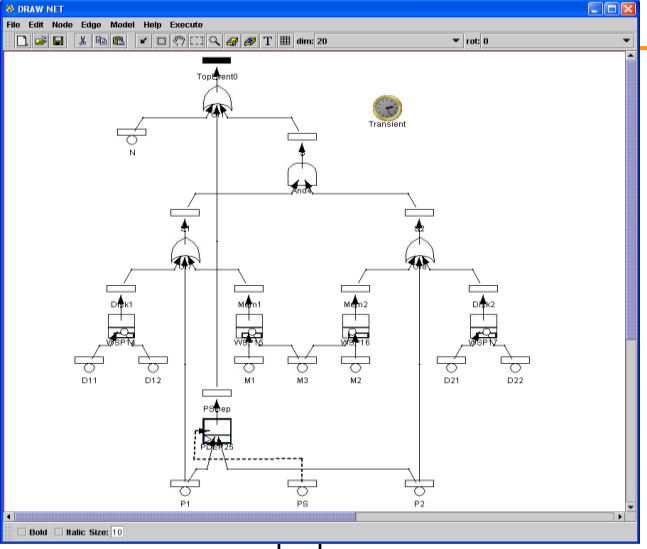
- A tool aimed at exploiting DBN inference for reliability purposes
- Automatic compilation of a DFT into a DBN
- Graphical User Interface (both for DFT and DBN)
- Filtering and Smoothing inference (1.5JT and BK algorithms)
- Developed at the Computer Science Dept. of U.P.O.

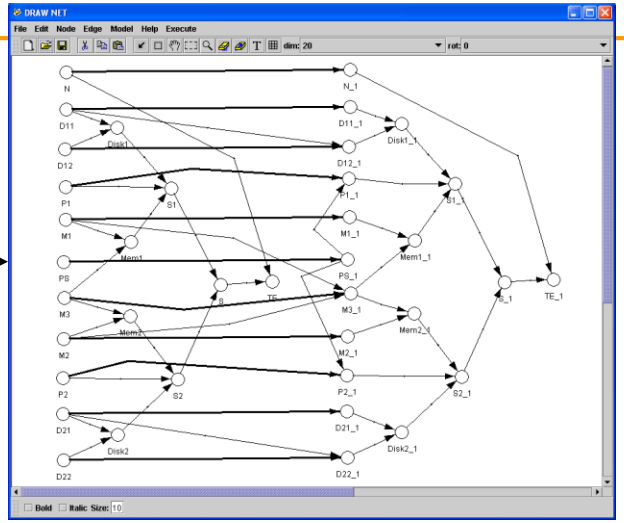
Available online at www.sciencedirect.com
ScienceDirect
Reliability Engineering and System Safety 93 (2008) 922–932

www.elsevier.com/locate/ress

RADYBAN: A tool for reliability analysis of dynamic fault trees through conversion into dynamic Bayesian networks

S. Montani, L. Portinale*, A. Bobbio, D. Codetta-Raiteri





DFT.xml

DFT2DBN

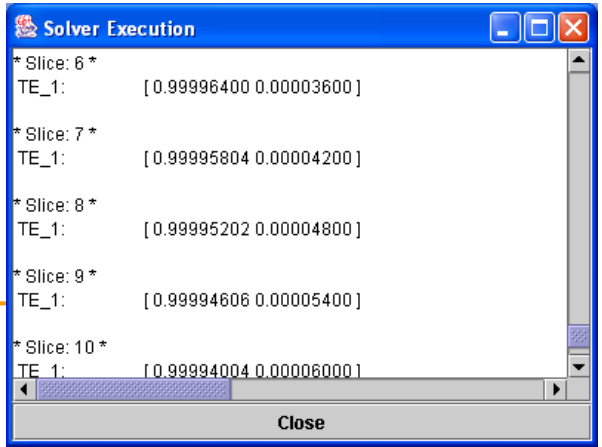
DBN.xml

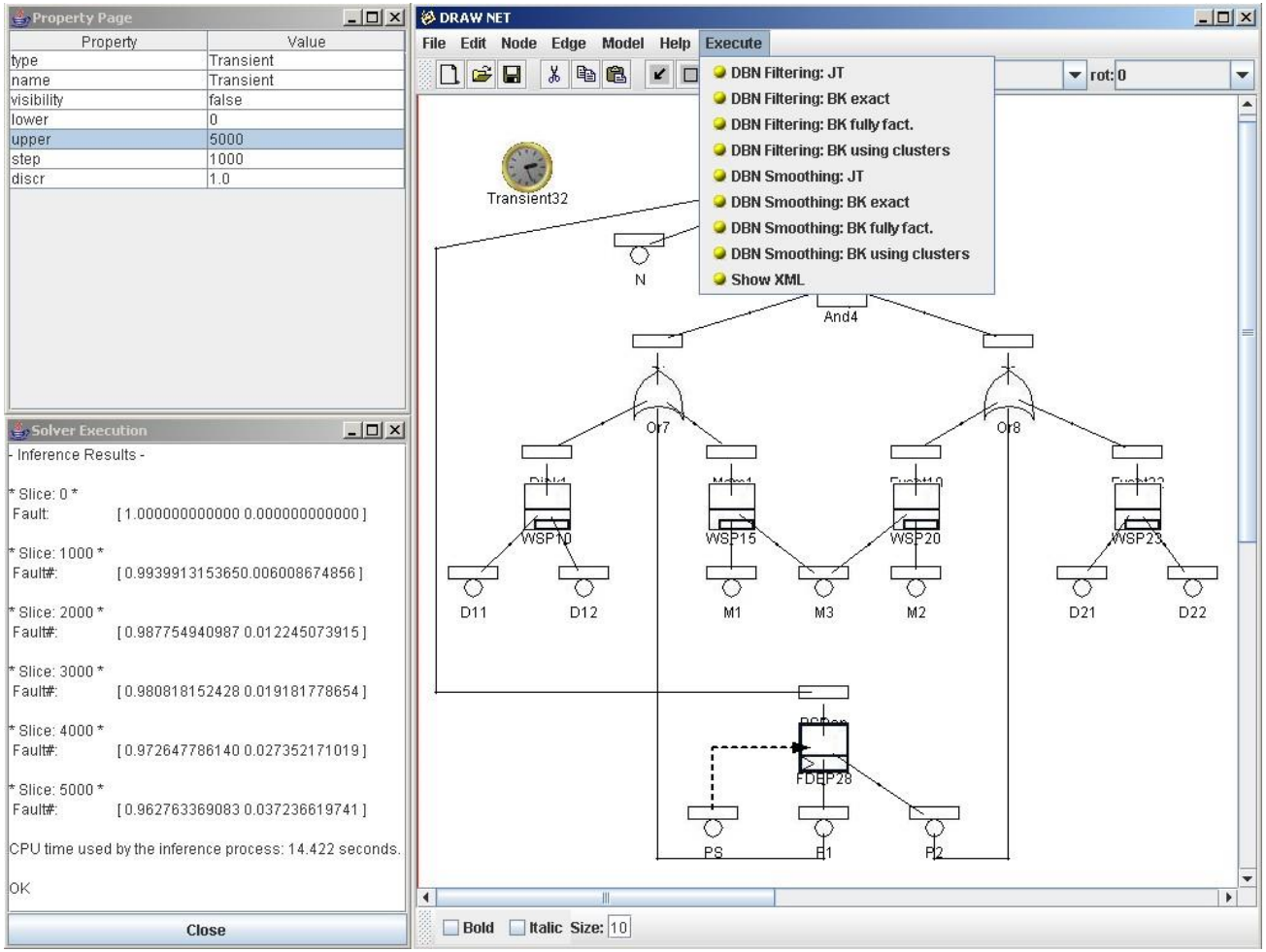
RADYBAN architecture and use

DBN analyzer

DBN.xml

Results





Draw-Net GUI
http://www.draw-net.com

INTEL PNL C++ libraries for DBN inference
http://sourceforge.net/projects/openpnl/

BN software tools

Open Issues

- Dealing with continuous variables
  - Gaussian Bayesian Networks
  - Hybrid Bayesian Networks
- Dealing with Continous Time
  - CTBN or GCTBN
- Making the formalism more tailored to reliability practitioners and analysts (tools, tools and … more tools)

Acknowledgments

- Colleagues
  - Prof. Andrea Bobbio
  - Prof. Stefania Montani
- Past Students
  - G. Vercellese
  - M. Varesio
  - S. Di Nolfo
- External collaborators
  - Ing. M. Minichino (ENEA)
  - Ing. E. Ciancamerla (ENEA)
  - Ing. A. Guiotto (Thales/Alenia)