Quantitative evaluation of non-Markovian stochastic models

Enrico Vicario
Lab. of Software Technologies - Dept. of Information Engineering - University of Florence
from joint work with: M.Biagi, L.Carnevali, A.Horvath, M.Paolieri

TU Wien - January 24, 2018

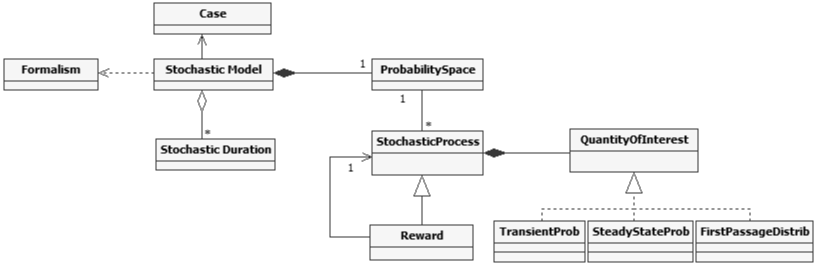
- this is about:
  - stochastic models and processes,... and non-Markovian processes,
  - and their quantitative evaluation
  - ... through the method of *stochastic state classes* and the *Oris tool*
  - with a few examples of application

- a technical talk interleaved with:
  - ground concepts of the research in *quantitative evaluation*

Outline

map of concepts: Models, Processes, and quantitative evaluation

- a model uses some formalism to capture a case in some reality
- a fully stochastic model identifies one single probability space
- ... on which we can define multiple stochastic processes and rewards
- ... amenable to solution to evaluate various quantities of interest



a few questions:

- what are models for?
  - early assessment of design choices
  - model driven guidance and insight
    for implementation, integration and operation stages
  - not only for SW intensive systems, but also for mechanics, physics, ...
    economics, social sciences, ... life sciences ...
- what is a stochastic model?
  - a *non-deterministic* model specifies an experiment allowing multiple outcomes
  - a *stochastic* model gives the space of outcomes a measure of probability
  - note: "stochastic" derives from the Greek word "stokhasticos", meaning able to guess, which in turn derives from "stokhos", meaning a stick target that an archer aims to shoot at
- why should a model be stochastic?
  - intrinsic stochastic behavior, by nature or by design
  - epistemic uncertainty, by abstraction
- what specific kind of stochastic model are we here dealing with ?
  - concurrent models
  - stochastic in choices e in durations
  - for systems that are supposed to meet real time requirements
    despite intertwined effects of concurrency and stochastic timing

more concretely, what is a model? and what is a formalism?

Kublai Khan: *But which is the stone that supports the bridge?*

Marco Polo: *The bridge is not supported by one stone or another,
but by the line of the arch that they form.*

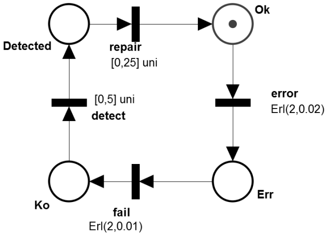
Kublai Khan: *Why do you speak to me of the stones?
It is only the arch that matters to me.*

Marco Polo: *Without stones there is no arch.*

Italo Calvino, Invisible Cities, 1978.

... about the Formalism and the Model - 1/2

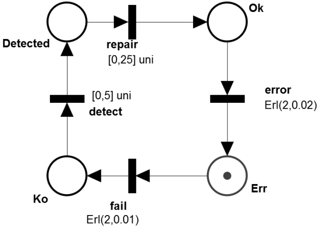
- stochastic Time Petri Nets (sTPN):
  a class of SPNs with generally distributed durations
  - places encode state conditions, true if at least one token
  - transitions encode events, enabled if all input conditions are true
  - at firing, move tokens from input to output places
    and sample a time to fire for each newly enabled transition
  - delay from enabling to firing is a random variable



- a cycle of two step failure, detection delay, repair and restart as new

... about the Formalism and the Model - 1/2

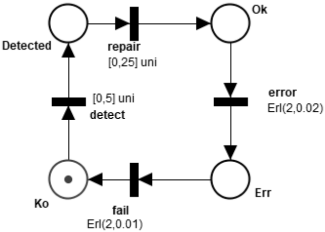
- stochastic Time Petri Nets (sTPN):
  a class of SPNs with generally distributed durations
  - places encode state conditions, true if at least one token
  - transitions encode events, enabled if all input conditions are true
  - at firing, move tokens from input to output places
    and sample a time to fire for each newly enabled transition
  - delay from enabling to firing is a random variable



- a cycle of two step failure, detection delay, repair and restart as new

... about the Formalism and the Model - 1/2

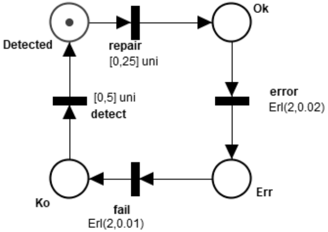
- stochastic Time Petri Nets (sTPN):
  a class of SPNs with generally distributed durations
  - places encode state conditions, true if at least one token
  - transitions encode events, enabled if all input conditions are true
  - at firing, move tokens from input to output places
    and sample a time to fire for each newly enabled transition
  - delay from enabling to firing is a random variable



- a cycle of two step failure, detection delay, repair and restart as new

... about the Formalism and the Model - 1/2

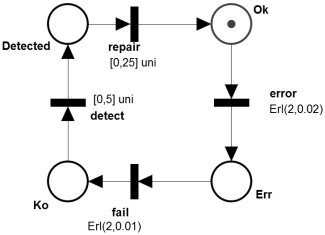
- stochastic Time Petri Nets (sTPN):
  a class of SPNs with generally distributed durations
  - places encode state conditions, true if at least one token
  - transitions encode events, enabled if all input conditions are true
  - at firing, move tokens from input to output places
    and sample a time to fire for each newly enabled transition
  - delay from enabling to firing is a random variable



- a cycle of two step failure, detection delay, repair and restart as new

... about the Formalism and the Model - 1/2

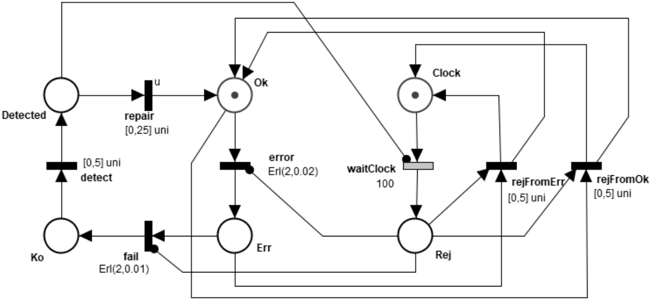
- stochastic Time Petri Nets (sTPN):
  a class of SPNs with generally distributed durations
  - places encode state conditions, true if at least one token
  - transitions encode events, enabled if all input conditions are true
  - at firing, move tokens from input to output places
    and sample a time to fire for each newly enabled transition
  - delay from enabling to firing is a random variable



- a cycle of two step failure, detection delay, repair and restart as new

... about the Formalism and the Model - 2/2

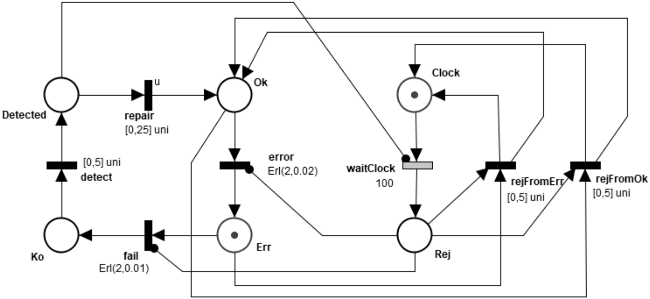
- ... compose with time-triggered rejuvenation to increase reliability[1]
- ... and to let concurrency appear



[1] (tweaked from:) S.Garg, A.Puliafito, M.Telek, K.S.Trivedi, "Analysis of software rejuvenation using Markov regenerative stochastic Petri net," Software Reliability Engineering, 1995.

... about the Formalism and the Model - 2/2

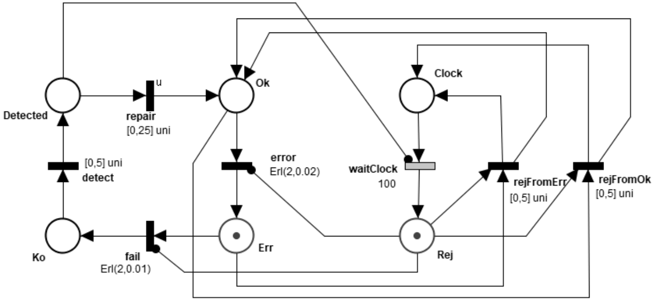
- ... compose with time-triggered rejuvenation to increase reliability[1]
- ... and to let concurrency appear



[1] (tweaked from:) S.Garg, A.Puliafito, M.Telek, K.S.Trivedi, "Analysis of software rejuvenation using Markov regenerative stochastic Petri net," Software Reliability Engineering, 1995.

... about the Formalism and the Model - 2/2

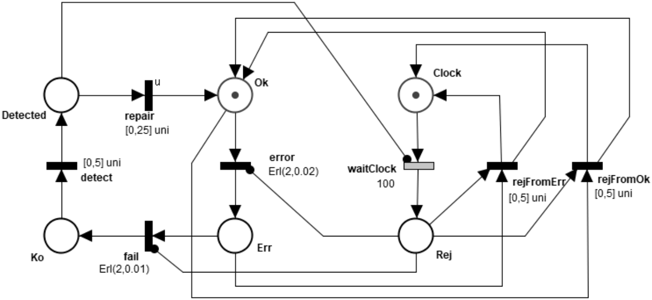
- ... compose with time-triggered rejuvenation to increase reliability[1]
- ... and to let concurrency appear



[1] (tweaked from:) S.Garg, A.Puliafito, M.Telek, K.S.Trivedi, "Analysis of software rejuvenation using Markov regenerative stochastic Petri net," Software Reliability Engineering, 1995.

... about the Formalism and the Model - 2/2

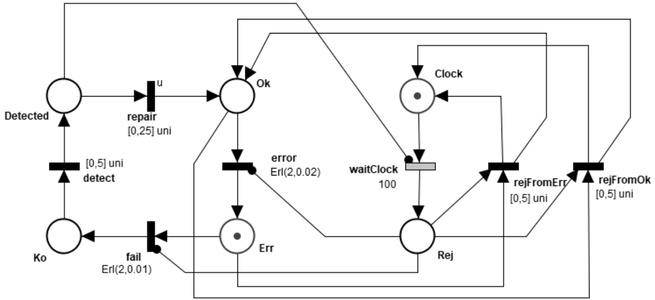
- ... compose with time-triggered rejuvenation to increase reliability[1]
- ... and to let concurrency appear



[1] (tweaked from:) S.Garg, A.Puliafito, M.Telek, K.S.Trivedi, "Analysis of software rejuvenation using Markov regenerative stochastic Petri net," Software Reliability Engineering, 1995.

... about the Formalism and the Model - 2/2

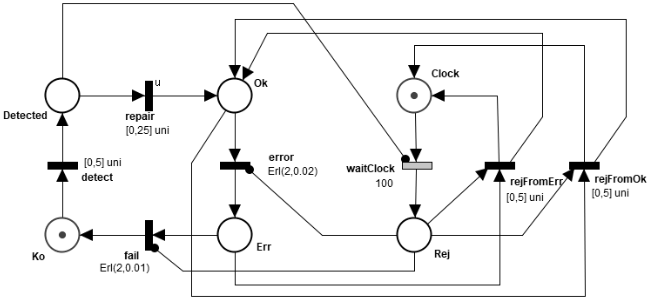
- ... compose with time-triggered rejuvenation to increase reliability[1]
- ... and to let concurrency appear



[1] (tweaked from:) S.Garg, A.Puliafito, M.Telek, K.S.Trivedi, "Analysis of software rejuvenation using Markov regenerative stochastic Petri net," Software Reliability Engineering, 1995.

... about the Formalism and the Model - 2/2

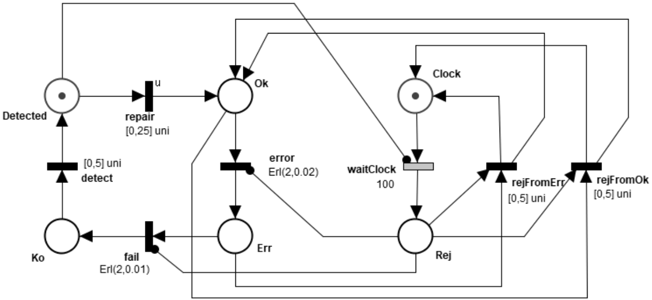
- ... compose with time-triggered rejuvenation to increase reliability[1]
- ... and to let concurrency appear



[1] (tweaked from:) S.Garg, A.Puliafito, M.Telek, K.S.Trivedi, "Analysis of software rejuvenation using Markov regenerative stochastic Petri net," Software Reliability Engineering, 1995.

... about the Formalism and the Model - 2/2

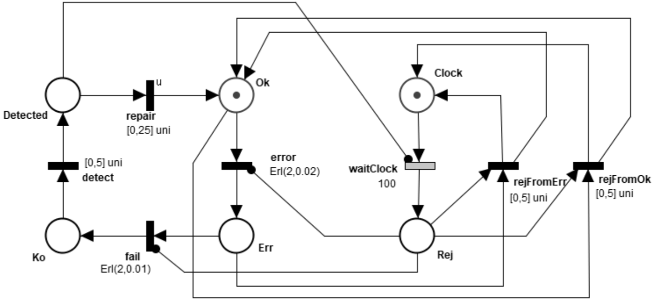
- ... compose with time-triggered rejuvenation to increase reliability[1]
- ... and to let concurrency appear



[1] (tweaked from:) S.Garg, A.Puliafito, M.Telek, K.S.Trivedi, "Analysis of software rejuvenation using Markov regenerative stochastic Petri net," Software Reliability Engineering, 1995.

... about the Formalism and the Model - 2/2

- ... compose with time-triggered rejuvenation to increase reliability[1]
- ... and to let concurrency appear



[1] (tweaked from:) S.Garg, A.Puliafito, M.Telek, K.S.Trivedi, "Analysis of software rejuvenation using Markov regenerative stochastic Petri net," Software Reliability Engineering, 1995.

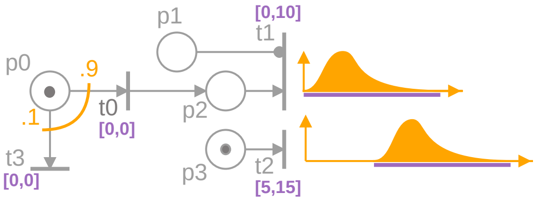
skip: details about stochastic Time Petri Nets (sTPN)

$$sTPN = \langle P, T, A^-, A^+, A^\bullet, m_0, \quad EFT, LFT, \tau_0, \quad \mathcal{F}, \mathcal{W} \rangle$$

(PN) concurrency, discrete locations, token moves:
places P, transitions T, initial marking m_0, arcs A^-, A^+, $A^\bullet$

(TPN) non-deterministic timed behavior, min-max durations, times to fire:
earliest and latest firing times EFT, LFT, initial times to fire τ_0

(sTPN) (fully) stochastic timed behavior:
probability density functions $\mathcal{F}$ for transition durations
discrete probabilities $\mathcal{W}$ for ties among transitions with equal time-to-fire



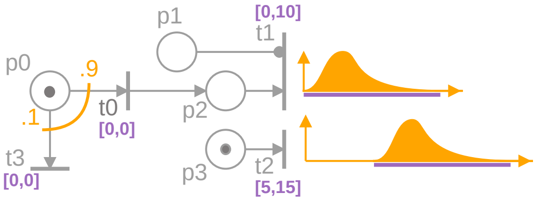
- ... and convenience extensions ... as usual

skip: details about the Probability Space, and its relation with the Formalism

- an sTPN (with an initial state) identifies a probability space

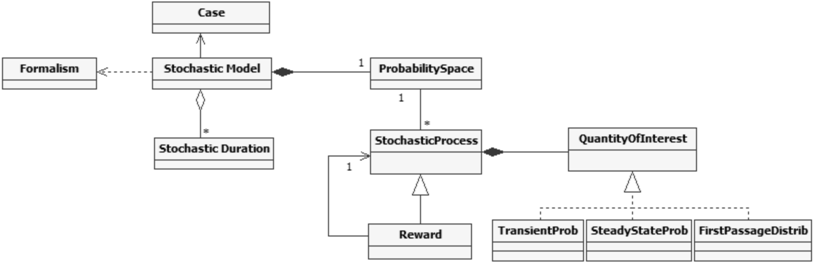
$$\langle \Omega, \mathcal{F}, \mathbb{P} \rangle$$

- the set of outcomes Ω is determined by the underlying TPN
  - (an outcome is an infinite run of the model)
  - Petri Net structure + duration supports
- the measure of probability $\mathbb{P}$ also depends on stochastic parameters
  - continuous distribution for transition firing times ($\mathcal{F}$)
  - discrete distribution for choices among transitions with equal firing times ($\mathcal{W}$)

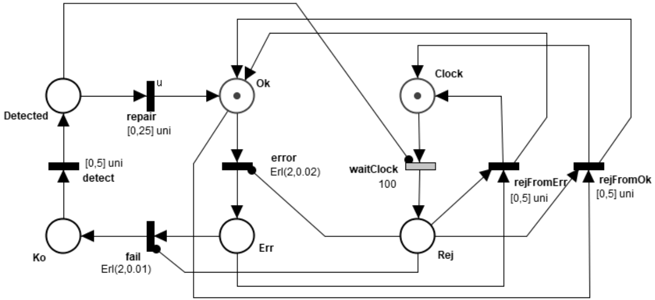


map of concepts: Models, Processes, and quantitative evaluation

- a model uses some formalism to capture a case in some reality
- a fully stochastic model identifies one single probability space
- ... on which we can define multiple stochastic processes and rewards
- ... amenable to solution to evaluate various quantities of interest



... about Stochastic Processes, and the marking process

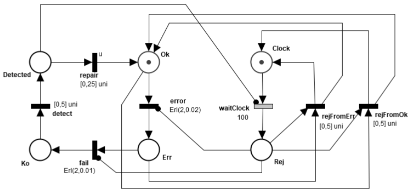


- a special underlying Stochastic Process: Marking Process

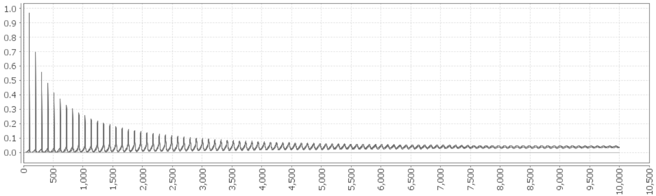
$$\mathbb{M} := \{M(t), t \in \mathbb{R}_{\geq 0}\}$$

- some Rewards: trade-off between Reliability and Availability
  - unReliability (*Ko*);
  - unAvailability (*Ko* $\vee$ *Detected* $\vee$ *Rej*);
  - "added" unAvailability
    (*Ok* $\wedge$ *Rej*).

... about Solution



- Rewards: unReliability (*Ko*); unAvailability (*Ko* ∨ *Detected* ∨ *Rej*); "added" unAvailability (*Ok* ∧ *Rej*)



question: what are we actually doing when we solve a Model?

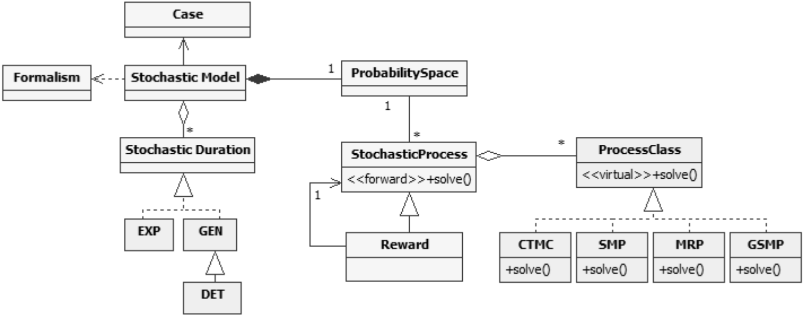
- the Model identifies a Probability Space

- a Reward specifies a Stochastic Process referred to the Marking Process
- ... so as to capture some Quantity of Interest for the Case

- and the Process is analyzed on the ground of mathematics
- ... using a SW tool

map of concepts: Durations and process Classes

- the underlying Stochastic Process of a Model is amenable to different solution techniques
- ... depending on its Class
- ... which in turn depends on the type of Durations and their concurrency



remark: which calls into play the Exponential Random Variable

- apparently, $EXP(\lambda)$ is just a Random Variable
  with exponential Probability Density Function (PDF):

$$f_X(t) = \lambda \cdot exp^{-\lambda \cdot t} \qquad t \in \mathbb{R}_{\geq 0}$$

- conversely, $EXP(\lambda)$ is uniquely marked by the *memoryless* property:

$$if\ X := EXP(lambda),\ \ Y := X|X > k,\ \ Z := Y - k \qquad THEN\ \ X = Z$$

- a direct consequence of a basic property of the exponential function:

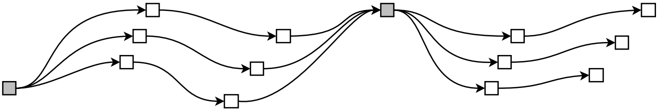
$$exp^{t_1+t_2} = exp^{t_1} * exp^{t_2}$$

- with major practical implications on expressivity and analyzability ...

remark: ... and the Markov Condition

- the Markov condition extends the memoryless property from Random Variables to Stochastic Processes
- "the future depends on the past only through the current marking"
  - so that prediction can get rid of the past history and its timing
- formally: the most recent observation of the marking m (at time t_0) subsumes any previous one (at times $t_{-1}, ...t_{-N}$):

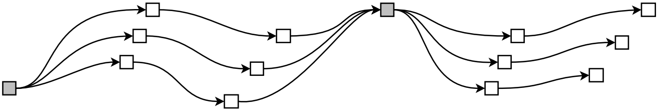
$$Prob\{m(t_1)|m(t_0)\} = Prob\{m(t_1)|m(t_0), m(t_{-1}), ...m(t_{-N})\}$$
$$\forall N, \quad \forall t_1 \geq t_0 \geq t_{-1} ... \geq t_{-N}$$



remark: on the overloaded meaning of the term "state"

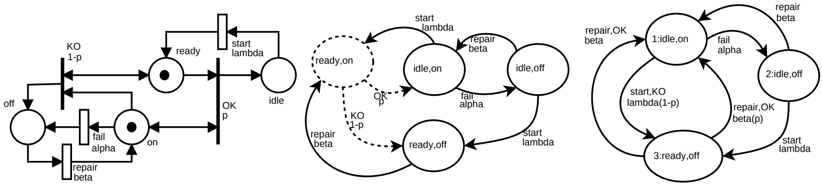
- in the operational semantics of a model,
  and more generally in most branches of Engineering
  state is any abstraction sufficient to get rid of the past history
- the state of a stochastic process is the value of "a" Random Variable,
- ... which in turn can be any function on the space of outcomes
- the Markov condition means: the process state is also a model state

- renewal argument: decompose a run across a time point
  (a kind of compositionality)



Continuous Time Markov Chain (CTMC)

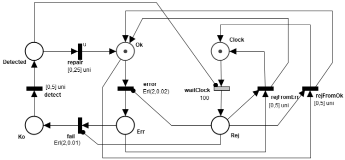
- if the model includes only IMM or EXP transitions,
  due to the memoryless property of EXP,
  the marking process always satisfies the Markov condition

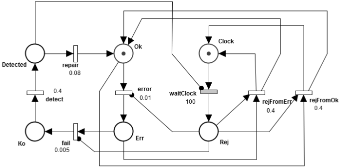


- the (right-continuous) marking process
  is thus a Continuous Time Markov Chain (CTMC)
  - characterized by a constant Infinitesimal Generator Q
  - solution through efficient and mature techniques

... about the Process Class: non-Markovian models

- ... but, models may include generally distributed (GEN) durations
  - break the limit of memoryless exponential (EXP) distributions
  - possibly with bounded support
  - (transition colors: white for EXP, black for GEN, gray for DET)

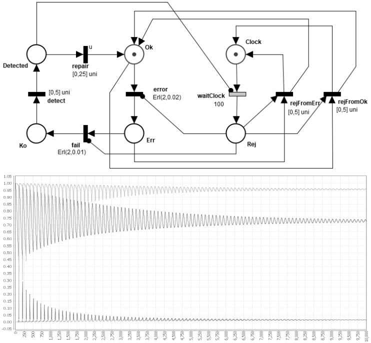


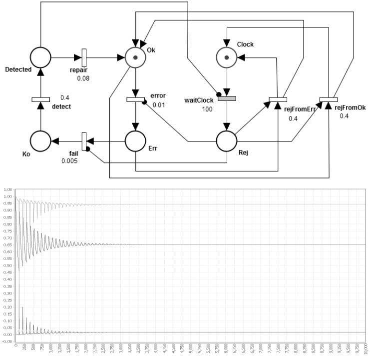


- may become relevant for validity in various application contexts
  - aging processes accumulating memory over time
  - real time systems with firm deadlines, bounded timeframes, synchronous releases, watchdogs, ...
  - timed protocols, signalling, ...

duration distributions matter - all EXP with DET clock

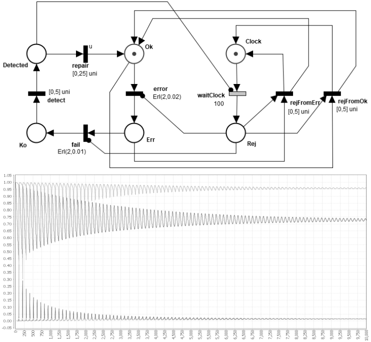
- change durations to EXP (with same mean), keeping the DET clock:

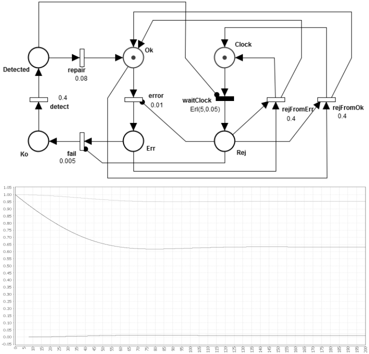




duration distributions matter - all EXP with Erl(5) clock

- if also the DET clock is changed into a sequence of 5 EXP (Erlang with the same expected value), ripples are completely lost

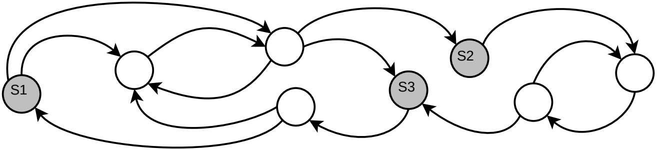




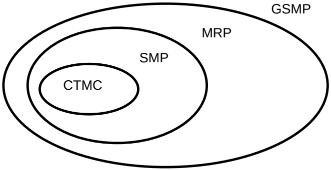
- (on the meaning of steady state and mixing time in a stochastic process)

Memory and regeneration

- if the model includes GEN transitions,
  the marking is in general not a sufficient model state
- yet, at some points,
  the marking can be sufficient to characterize future behavior
- call these *regeneration points*



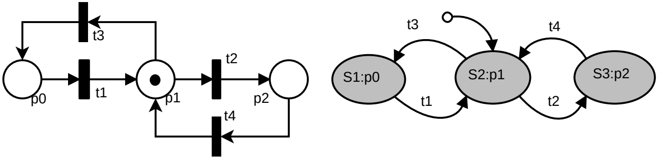
- the process class depends on how regeneration points are encountered[2]



[2] GF.Ciardo, R.German, C.Lindemann, "A characterization of the stochastic process underlying a stochastic Petri net," IEEE TSE, 1994.

Semi-Markov Process (SMP) -1/2

- if GEN transitions never persist through any firing
  the underlying stochastic process regenerates at every step
  (yet, memory is accumulated during sojourn)



- Global Kernel $G_{ij}(t)$: the first step from i is before t and reaches j

$$t_1 := \text{time of the first step}$$
$$G_{ij}(t) := Prob\{(t_1 < t) \wedge (m(t_1) = j) | m(t_0) = i \wedge t_0 = 0\}$$

- Holding time $H_i(t)$: the first step from i is after t

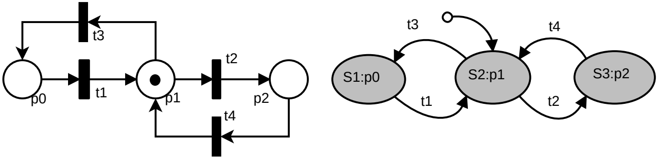
$$H_i(t) := Prob\{t_1 > t | m(t_0) = i \wedge t_0 = 0\}$$

- solved through a set of Volterra integral equations of the 2nd type:

$$\pi_{ij}(t) = H_i(t) \cdot \delta_{ij} + \sum_k \int_0^t \frac{dG_{ik}(x)}{dx} \pi_{kj}(t-x)dx$$

Semi-Markov Process (SMP) - 2/2

- global kernel and holding time derived directly from the model



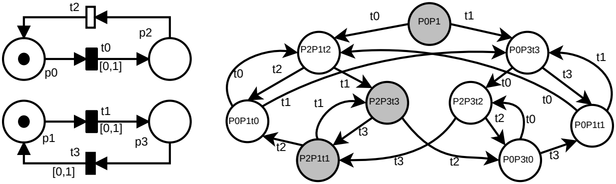
$$H(t) = \begin{pmatrix} 1 - F_1(t) \\ (1 - F_3(t)) \cdot (1 - F_2(t)) \\ 1 - F_4(t) \end{pmatrix}$$

$$G(t) = \begin{pmatrix} 0 & F_1(t) & 0 \\ \int_0^t f_3(x)(1 - F_2(x))dx & 0 & \int_0^t f_2(x)(1 - F_3(x))dx \\ 0 & F_4(t) & 0 \end{pmatrix}$$

- ... and Volterra equation solved by numerical integration
- but, no memory across subsequent locations

Markov Regenerative Process (MRP)

- always, wp1, the process eventually reaches a regeneration (possibly through infinite steps or in unbounded time)



- much more expressive, and actually sufficient for most purposes

MRP: kernels and generalized Markov renewal equations

- an MRP is characterized by 2 kernels $L(t)$ and $G(t)$
- Local Kernel $L_{ih}(t)$:
  starting from i, at t the state is h, and no regeneration occurred yet

$$t_1 := \text{time of the first regenertion}$$
$$L_{ih}(t) := Prob\{(t_1 > t) \wedge (m(t) = h) | m(t_0) = i \wedge t_0 = 0\}$$

- Global Kernel $G_{ij}(t)$:
  starting from i, the first regeneration is before t and leads to j

$$G_{ij}(t) := Prob\{(t_1 < t) \wedge (m(t_1) = j) | m(t_0) = i \wedge t_0 = 0\}$$

- transition probabilities can be derived by numerical integration of a set of integral equations (Volterra, 2nd type)

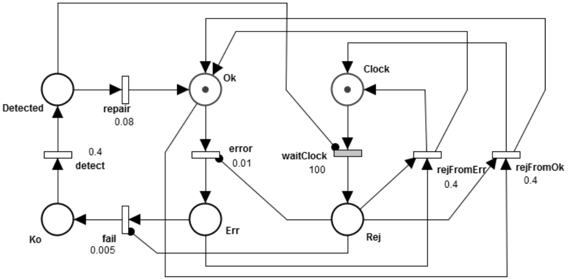
$$\pi_{il}(t) = L_{il}(t) + \sum_k \int_0^t \frac{dG_{ik}(x)}{dx} \pi_{kl}(t-x)dx$$

(generalized Markov renewal equations)

- ... but, how to get the kernels?

MRP: the special case of the enabling restriction

- if at most one GEN transition is enabled in any tangible marking
  - GEN transitions never persist to each other
  - the process subordinated to the activity period of a GEN is a CTMC, and kernels can thus be evaluated by uniformization [3] [4] [5]



- ... but, bad news for expressivity: no concurrent overlapping GEN timers

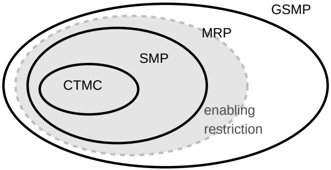
[3] GF.Ciardo, R.German, C.Lindemann, "A characterization of the stochastic process underlying a stochastic Petri net," IEEE TSE, 1994.

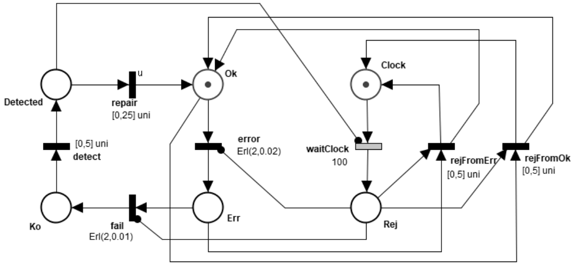
[4] A.Bobbio, M.Telek, "Markov regenerative SPN with non-overlapping activity cycles,"IPDS95.

[5] H.Choi, V.G.Kulkarni, K.S.Trivedi, "Markov Regenerative stochastic Petri Nets," PEVA'94.

on the frontier of MRP

- the class of MRP is much wider than the enabling restriction



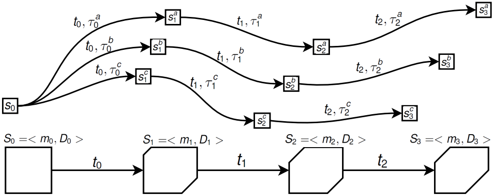


a "recent" approach

- the method of *stochastic state classes*
  - multiple concurrent GEN, possibly over bounded supports
  - best fitting the case of "bounded regeneration"
- main concepts
  - compute probability densities over DBM zones
    that represent continuous sets of reachable states
  - add an age clock to enable transient analysis
  - restrain transient analysis within regeneration epochs,
    to evaluate local and global kernels,
    and then resort to Markov Renewal Theory
- implemented in the Oris tool and API

a step back to the underlying non-deterministic TPN

- a finite sequence of transitions $\rho := s_0 : t_0 \rightarrow t_1 \ldots \rightarrow t_n$ can be executed with a continuous multivariate set of timings $\{\tau_1, \tau_2 \ldots \tau_n\}$



- call *state class* S_n the set of states reached after n steps along ρ
  - a common marking m_n, but a set D_n of different vectors of remaining times
  - the set D_n has the shape of a Difference Bounds Matrix (DBM) Zone [6] [7] [8] [9]
  - efficient (polynomial) symbolic encoding and manipulation

---

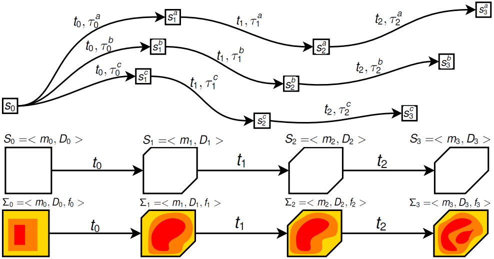
[6] D. L. Dill, "Timing assumptions and verification of finite-state concurrent systems," 1989

[7] B.Berthomieu,M.Diaz,"Modeling and verification of time dependent systems using TPNs"TSE91.

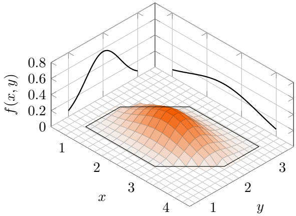
[8] J. Bengtsson, K. Larsen, F. Larsson, P. Pettersson, and W. Yi, "UPPAAL - A tool suite for automatic verification of real-time systems," 1996.

[9] E.Vicario,"Static Analysis and Dynamic Steering of Time-Dependent Systems Using TPNs,"TSE01

compute probabilities over DBM zones



- stochastic state class $\Sigma =< M, D, f() >$
  - decorates each state class $< M_n, D_n >$ with the joint prob. density function $f_n()$ of times to fire of enabled transitions, as observed when the class is entered

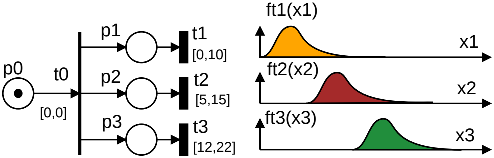


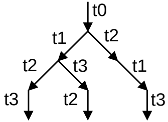
10

[10] E.Vicario, L.Sassoli, L.Carnevali, "Using Stochastic State Classes in Quantitative Evaluation of Dense-Time Reactive Systems", IEEE TSE 2009

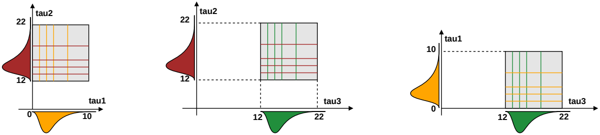
skip: calculus of stochastic classes - 1/2

- assume that transitions are initially newly enabled



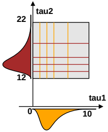


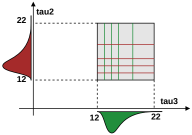
- ... their times to fire are distributed independently,
  in product form, according to their static density function

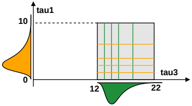


skip: calculus of stochastic classes - 2/2

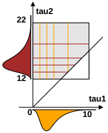
- starting from a product form over a hyper-rectangle ...



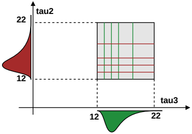


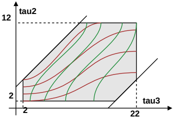


- ... the assumption that t_1 fires first
  restricts the support and uniformly conditions probabilities



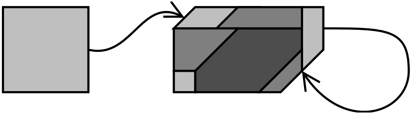
- ... at the firing of t_1, a random time has elapsed
  - remaining times to fire of persistent transitions t_2 and t_3 become dependent, and supported over a Difference Bounds Matrix (DBM) zone





calculus of stochastic classes

- when subsequent transitions occur,
  supports remain in the shape of a Difference Bounds Matrix (DBM) zone
  - density functions are continuous piecewise multivariate functions
    over a partition in DBM sub-zones, continuous across internal borders



- closed form symbolic derivation for models with EXP, IMM, DET,
  and ExPol transitions (with possibly bounded support) [11]

$$f_t^s(x) = \sum_k^K c_k x^{\alpha_k} e^{-\lambda_k x} \quad \text{for } x \in [EFT_t^s, LFT_t^s,]$$

- implementation amounts to joint symbolic enumeration of DBM domains
  and analytical form of multi-variate joint density functions
  - intertwining due to zone difference constraints (linear, slope 1)

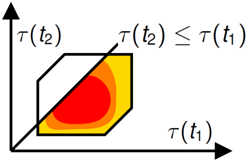
[11] L.Carnevali, L.Grassi, E.Vicario, "State-density functions over DBM domains in the analysis of non-Markovian models," TSE'09.

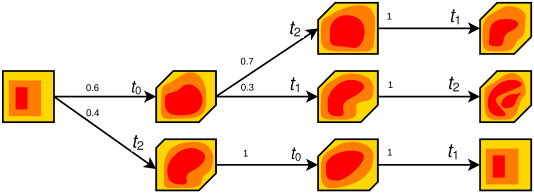
measures enabled by stochastic state classes

- the probability that t_2 fires first (transition probability) is the integral over a DBM subset of the DBM zone

$$Prob\{t_1 \ fires\} = \int_{D \wedge (\tau(t_2) \leq \tau(t_n) \ \forall n)} f_{\underline{\tau}}(\underline{x}) d\underline{x}$$

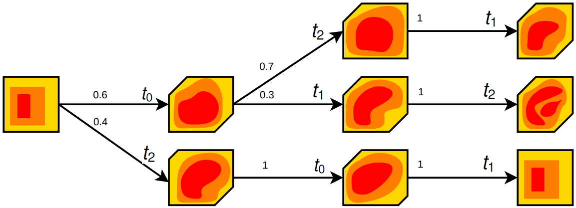
- the probability to reach a class is the product of transition probabilities on the path from the root





... use state classes as a measure of probability over the set of runs

- tree of stochastic state classes
  - explicit representation for the measure of probability over sets of runs [12]
  - discrete probability to reach a class
  - continuous probability measure
    over any subset of remaining times when the class is reached



- characterizes the process at the time when a class is entered
  - characterization w.r.t. absolute time when the class is reached
    obtained by supplementing classes with a global age variable [13]

[12] M.Paolieri, A.Horváth, E.Vicario "Probabilistic Model Checking of Regenerative Concurrent Systems," accepted, IEEE Trans. on Software Engineering, Feb. 2016.

[13] A.Horváth, M.Paolieri, L.Ridi, E.Vicario, "Transient analysis of non-Markovian models using stochastic state classes," PEva, 2012.

measures enabled by transient stochastic state classes

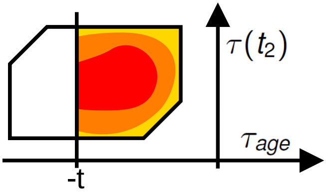
- probability that class S is reached within time t:

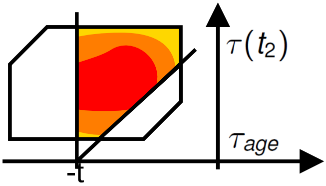
$$\pi_S \cdot \int_{D \wedge -x_{age} \leq t} f_{\langle \tau_{age}, \underline{\tau} \rangle}(x_{age}, \underline{x}) dx_{age} d\underline{x}$$

- probability that S is the last entered class at time t
(S is reached within $u \leq t$, the sojourn time is not lower than $t - u$)

$$\pi_S(t) = \pi_S \cdot \int_{D(t)} f_{\langle \tau_{age}, \underline{\tau} \rangle}(x_{age}, \underline{x}) dx_{age} d\underline{x}$$

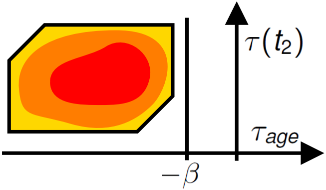
$$D(t) = D \wedge (-x_{age} \leq t) \wedge (-x_{age} + Min_n\{x_n\} \geq t)$$





transient analysis straight through the probability measure

- a straight approach to transient analysis:
  - enumerate classes until the time horizon is overcome
  - not only for MRP, also for GSMP



- fairly general termination conditions
  - exact analysis terminates iff the non-deterministic SCG does not reach within time T any *possibly immediate* cycle
  - analysis with safe approximation $\epsilon > 0$ terminates iff the non-deterministc SCG does not reach within time T any *necessarily immediate* cycle (time block)
- yet, the transient stochastic tree grows exponentially with the number of transition firings within the scope of transient analysis

combine stochastic state classes with Markov renewal theory

- restrain transient analysis within the first epoch
  use it to evaluate local and global kernels,
  and then resort to Markov Renewal Theory for MRPs
- derive kernels through measures on enumerated classes
  - local kernel: starting from i, at time t the marking is j and no regeneration has occurred

$$L_{ih}(t) := Prob\,(t_1 > t \wedge m(t) = h | m(t_0) = i \wedge t_0 = 0)$$

  - global kernel: starting from i, the first regeneration is before t and leads to j

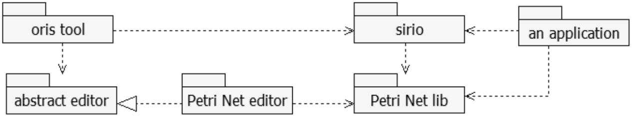
$$G_{ij}(t) := Prob\,(t \geq t_1 \wedge m(t_1) = j | m(t_0) = i \wedge t_0 = 0)$$

- get transient probabilities through generalized Markov renewal equations

$$\begin{aligned}
\pi_{il}(t) &:= Prob\{m(t) = l | m(0) = i\} \\
\pi_{il}(t) &= L_{il}(t) + \sum_k \int_{x=0}^{t} \frac{dG_{ik}}{dx}(x)\pi_{kl}(t-x)dx
\end{aligned}$$

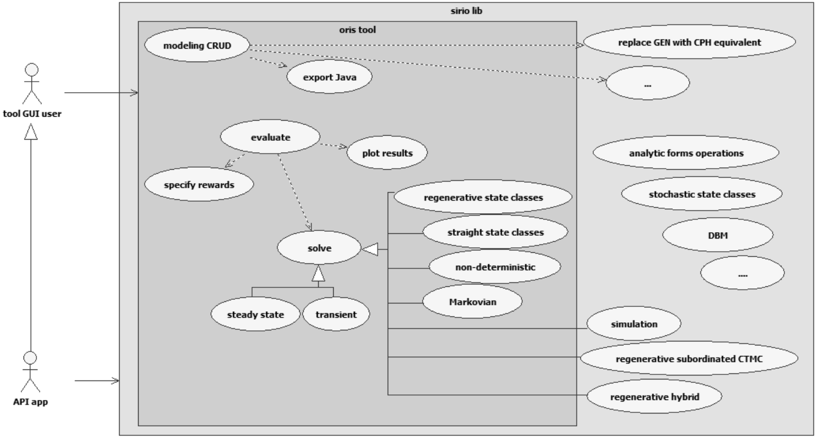
analysis in the Oris tool

- full Java implementation in the Oris tool [14]
  - rich extension of sTPN
  - approximation allowed
  - rewards
  - various analysis techniques
  - ... much more in the API
- underlying implementation also available, with many more functions
  - Sirio: symbolic calculus of PDF over DBM
  - PetriNetLib: syntax and semantics of Petri Nets, easily open to extensions
  - abstractEditor: a customizable framework for the production of graph-based formalisms

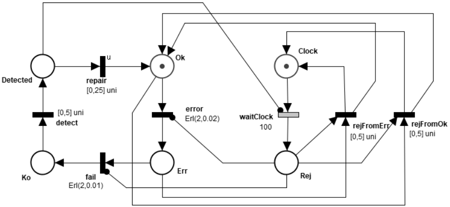


[14] http://www.oris-tool.org/

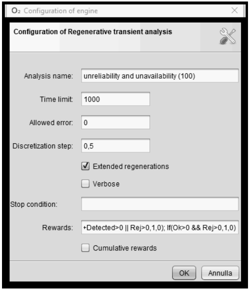
map of concepts: The Oris tool and the Sirio library

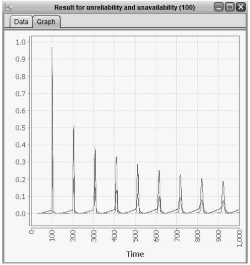


unavailability and unreliability

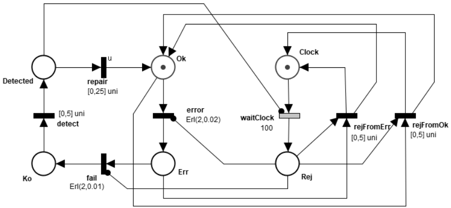


- unreliability: Ko
- unavailability:
  Ko>0 || Detected>0 || Rej>0
- added unavailability:
  Ok>0 && Rej>0

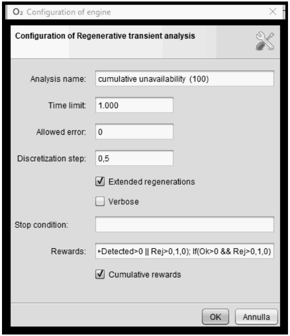


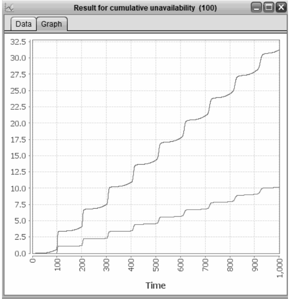


unavailability - cumulative

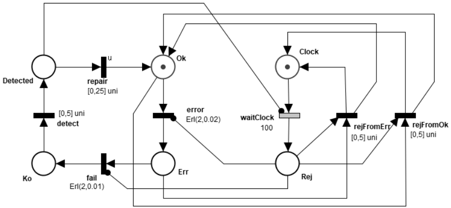


- unavailability:
  Ko>0 || Detected>0 || Rej>0
- added unavailability:
  Ok>0 && Rej>0

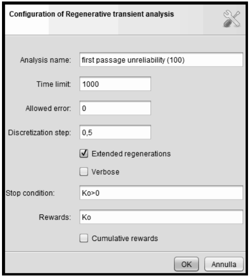


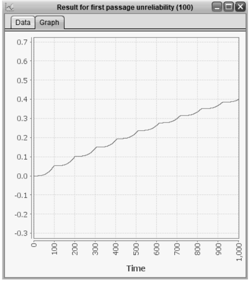


unreliability - first passage time

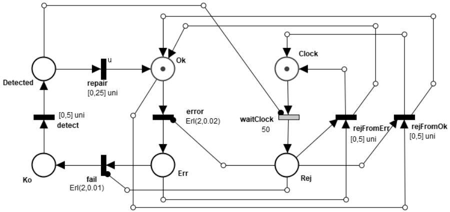


- unreliability: Ko>0

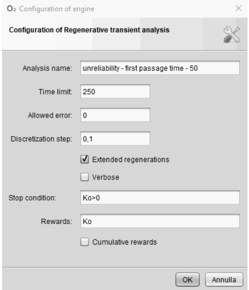


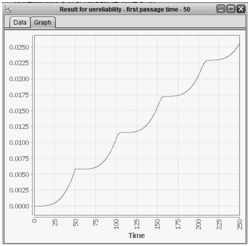


unreliability - first passage time - 50

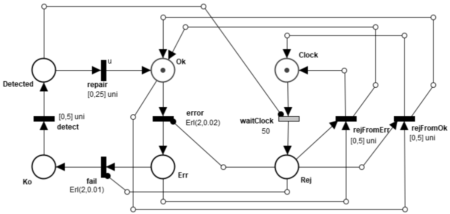


- unreliability: Ko>0

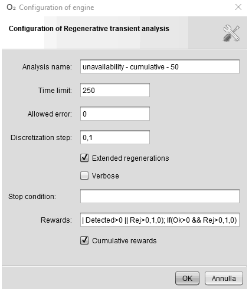


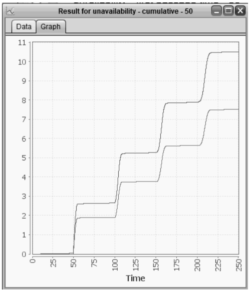


unavailability - cumulative - 50



- unavailability:
  Ko>0 || Detected>0 || Rej>0
- added unavailability:
  Ok>0 && Rej>0



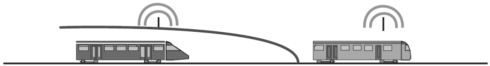


... some experiments of application

- dependability/performance evaluation of ...
  - performability evaluation for ERTMS/ETCS-level3
  - recoverability and serviceability in gas distribution networks
  - ... and water distribution networks
- on-line implementation as smart component of ...
  - Activity Recognition (AR) in Ambient Assisted Living (AAL)

performability evaluation for ERTMS/ETCS-level3

- impact of communication (un)availability in headway control for a chasing train in the RTCS level-3 signalling standard [15]
  - trade off between headway distance (capacity) and breaking probability



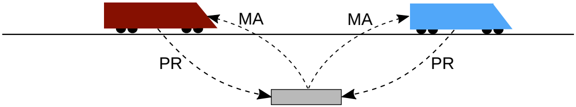
- a transient problem, with multiple concurrent GEN durations
  - previous works on steady state, and under enabling restriction[16]

[15] M. Biagi, L. Carnevali, M. Paolieri, and E. Vicario, "Performability evaluation of the ERTMS/ETCS - Level 3", Transportation Research Part C: Emerging Technologies,Sept.2017.

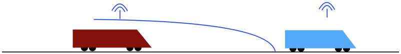
[16] A.Zimmermann, G.Hommel,"Towards modeling and evaluation of ETCS realtime communication and operation," Journal of Systems and Software, 2005

European Rail Traffic Management System (ERTMS)

- ERTMS: standard for train signalling and traffic management
- based on the European Train Control System (ETCS)
  - Automatic train protection system for continuous train supervision
  - A trackside equipment receives a periodic Position Report (PR) for each supervised train and sends back a Movement Authority (MA)
  - A train triggers an emergency brake if the allowed speed is exceeded

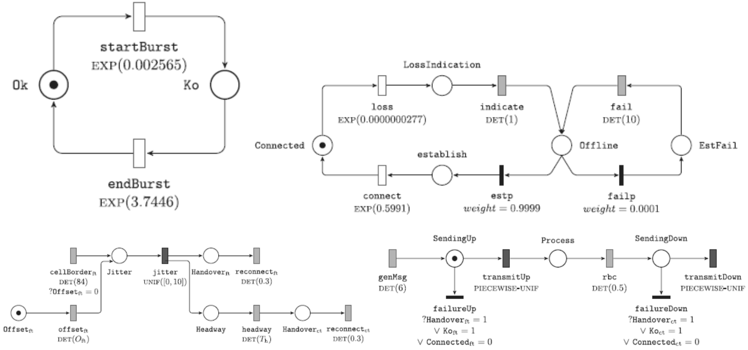


- ERTMS/ETCS Level 3 of operation
  - Moving-block signalling:
    trains check position and integrity autonomously
  - No train detection systems:
    installation/maintenance savings, capacity gains
  - Mobile communication is key: trade-off between capacity and false alarms



first-passage time distribution to emergency brake due to GSM-R failures

- GSM-R failures due to burst noise, connection losses, handovers composed with a model of periodic transmission of PRs and MAs [17]
  - Non-Markovian models specified through Stochastic Time Petri Nets (STPN)
  - Periodic handovers of a pair of chasing trains are dependent events
  - Stochastic parameters from Zimmermann et al (2003, 2005), and amendments in the evolution of the ERTMS/ETCS specification



[17] M. Biagi, L. Carnevali, M. Paolieri, and E. Vicario, "Performability evaluation of the ERTMS/ETCS - Level 3", Transportation Research Part C: Emerging Technologies, Sept.2017.

combination of analytic evaluation and transient analysis

- Stochastic evaluation of the flat model would be practically not feasible
  - Transient analysis via the ORIS Tool (`http://www.oris-tool.org`) [18] would suffer the many concurrent timers with general (GEN) distribution
  - Approaches based on the approximation of GEN transitions [19] [20] [21]
  - Simulation would suffer rare events, different order of magnitude of durations
- GSM-R failures are due to independent phenomena
- GSM-R unavailability is evaluated separately for each failure type either analytically or through transient analysis via the ORIS Tool
  - Multiple losses due to burst noise can be regarded as independent events
  - Connection losses negligibly affect the GSM-R availability wrt burst noise
  - At most 2 out of 4 consecutive PRs and/or MAs can be lost due to handovers
- Evaluation within 2 hyper-periods yields an upper-bound on the first passage time distribution to an emergency brake in an unbounded interval

[18] A.Horváth, M.Paolieri, L.Ridi, E.Vicario, Transient analysis of non-Markovian models using stochastic state classes. Performance Evaluation, 2012.

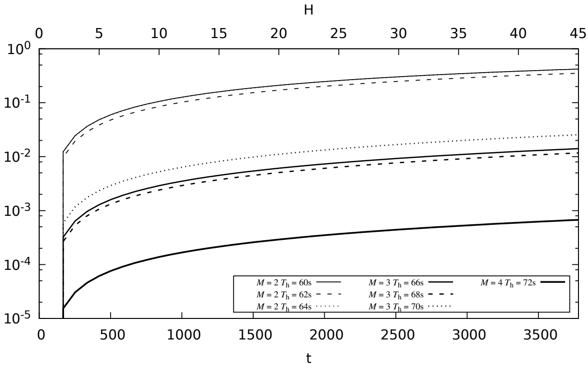
[19] A.Horvath, A.Puliafito, M.Scarpa, M.Telek, Analysis and Evaluation of non-Markovian Stochastic Petri Nets. Int. Conf. on Computer Performance Evaluation, 2000.

[20] F.Longo, M.Scarpa, Applying Symbolic Techniques to the Representation of Non-Markovian Models with Continuous PH Distributions. EPEW, 2009.

[21] C.Lindemann, A.Thümmler, Transient analysis of deterministic and stochastic Petri nets with concurrent deterministic transitions. Performance Evaluation, 1999

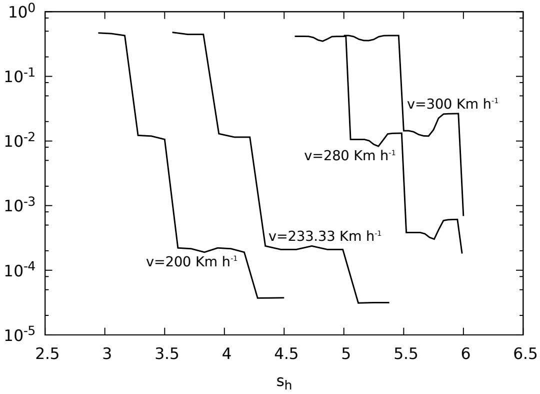
Upper-bound on first-passage time distribution to emergency brake due to GSM-R failures - 1/2

- Upper-bound on the first-passage probability that an emergency brake occurs within H hyper-periods, computed for different headway delays T_{h}
  - The duration of a hyper-period is 84 *sec* $\Rightarrow$ 45 hyper-periods $\sim$ 1*hour*
  - The train speed is 300 $Km/hour$



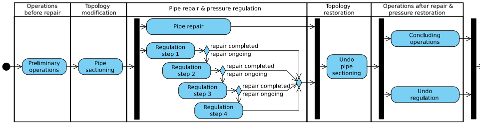
Upper-bound on first-passage time distribution to emergency brake due to GSM-R failures - 2/2

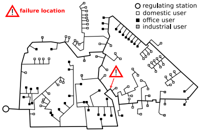
- Upper-bound on the first-passage probability that an emergency brake occurs within 45 hyper-periods ($\sim$ 1 *hour*) as a function of the headway distance s_h (expressed in *km*), computed for different values of speed v



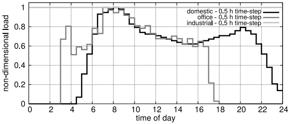
Recoverability and serviceability in gas distribution networks

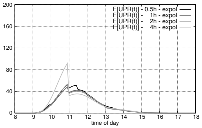
- Gas distribution networks couple physical fluid-dynamic processes with cyber management procedures [22] [23] [24]

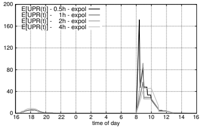




- Goal: evaluate the low pressure risk in the transient phase after a repair, due to a contingency or a planned operation of pipe sectioning







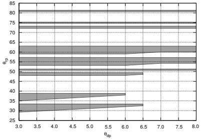
[22] M. Biagi, L. Carnevali, F.Tarani, E. Vicario, “Model-based quantitative evaluation of repair procedures in gas distribution networks”, submitted to ACM Transactions on Cyber-Physical Systems.

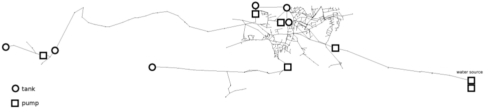
[23] L. Carnevali, M. Paolieri, F. Tarani, E. Vicario, and K. Tadano, "Modeling and evaluation of maintenance procedures for gas distribution networks with time-dependent parameters", in Int. Workshop on Reliability and Security Aspects for Critical Infrastructure Protection (ReSA4CI), 2014.

[24] L. Carnevali, M. Paolieri, K. Tadano, and E. Vicario, "Towards the Quantitative Evaluation of Phased Maintenance Procedures Using Non-Markovian Regenerative Analysis", in European Performance Engineering Workshop (EPEW), 2013.

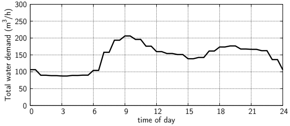
Recoverability and serviceability in *water* distribution networks

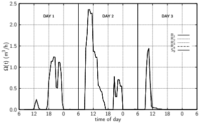
- A more complex and different problem than what might appear, formulated with reference to the class of stochastic hybrid systems [25]
  - Water distribution networks feature a continuous and discrete dynamics (with the water level in tanks comprising a continuous element of memory)
  - Topology and operation mode can be changed at stochastic time points





- Goal: evaluate the expected demand not served in the time after a repair

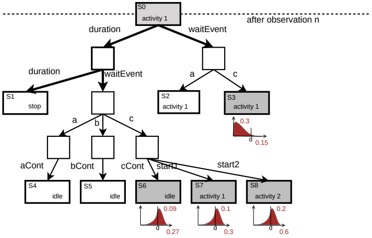




[25] L. Carnevali, F. Tarani, E. Vicario, "Performability evaluation of water distribution systems during maintenance procedures", IEEE Transactions on Systems, Man, and Cybernetics: Systems, accepted for publication.

Activity Recognition (AR) in Ambient Assisted Living (AAL)

- A problem of diagnosis in a partially-observable system [26] [27]
  - A stochastic model is rejuvenated by runtime observations
  - Transient probabilities computed on the model@runtime provide a likelihood for the diagnosis of the current state



- A kind of continuous-time extension of Hidden Markov Models (HMMs)
  - Exploiting the conditionment of the observation of times between events
  - Relevant only in non-Markovian systems

[26] M. Biagi, L. Carnevali, M.Paolieri, F. Patara, E. Vicario, "A continuous-time model-based approach for activity recognition in pervasive environments", submitted to IEEE Transactions on Human-Machine Systems.

[27] L. Carnevali, C. Nugent, F. Patara, E.Vicario, "A continuous-time model-based approach to activity recognition for ambient assisted living", in International Conference on Quantitative Evaluation of SysTems (QEST), pp. 38-53, 2015.

... from diagnosis towards prediction and scheduling

- starting from each plausible current state,
  compute the distribution of the hitting time of some critical state
- schedule the time point of some typed action
  - in the AAL setting: schedule monitoring escalation or warnings
  - applicable to a variety of scenarios with a sensing and actuation infrastructure
- a tailored application giving value to
  effective evaluation of transient behavior

a few closing remarks:

- much more to be done in the solution of non-Markovian models
  ... and large potential of application of existing tools
- about verification vs evaluation
  and qualitative (non-deterministic) vs quantitative (stochstic)
- about verification of Real Time constraints on Markovian models
  - systems with real time requirement natively include firm timing mechanisms (e.g. timeouts, watchdogs, periodic releases, bounded execution times)
  - which break the assumptions of memoryless and unbounded behavior of EXP variables,
  - and require representation of generally distributed (GEN) durations
  - not always enabling clean mathematics but relevant for engineering
- about quantitative evaluation and model-based approaches
  in the age of big data and machine learning