A Modeling Approach to Analyze the Impact of Error Propagation on Reliability of Component-based Systems

Vittorio Cortellessa*   Vincenzo Grassi**

*Università dell'Aquila, Italy
**Università di Roma "Tor Vergata", Italy

Predictive analysis of component-based systems

- Useful *to drive* the design process (*what if* analysis)
  - selection and composition of components
  - identification of critical components
- late problem fixing may be too costly

- Predictive analysis must be carried out on ***models*** of the system!

- **Analytic models** are good candidates for predictive analysis

quick analysis results, sensitivity analysis by analytic tools

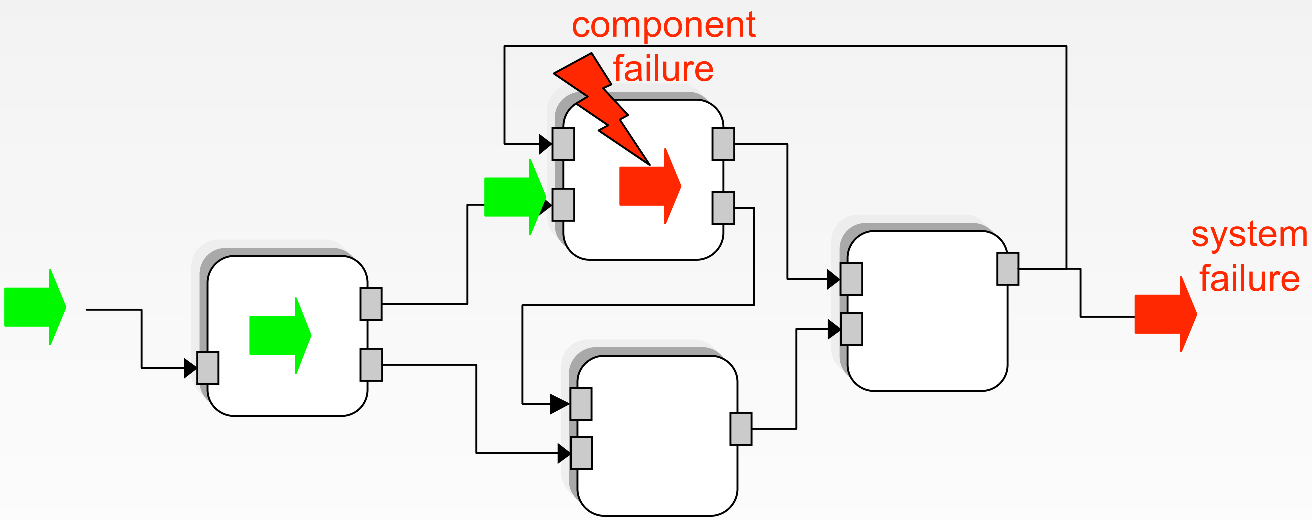
but ...

risk of excessive oversimplifications (and misleading results)

- Our focus is on **analytic models** for **reliability** analysis of C-B systems

Reliability of component-based systems

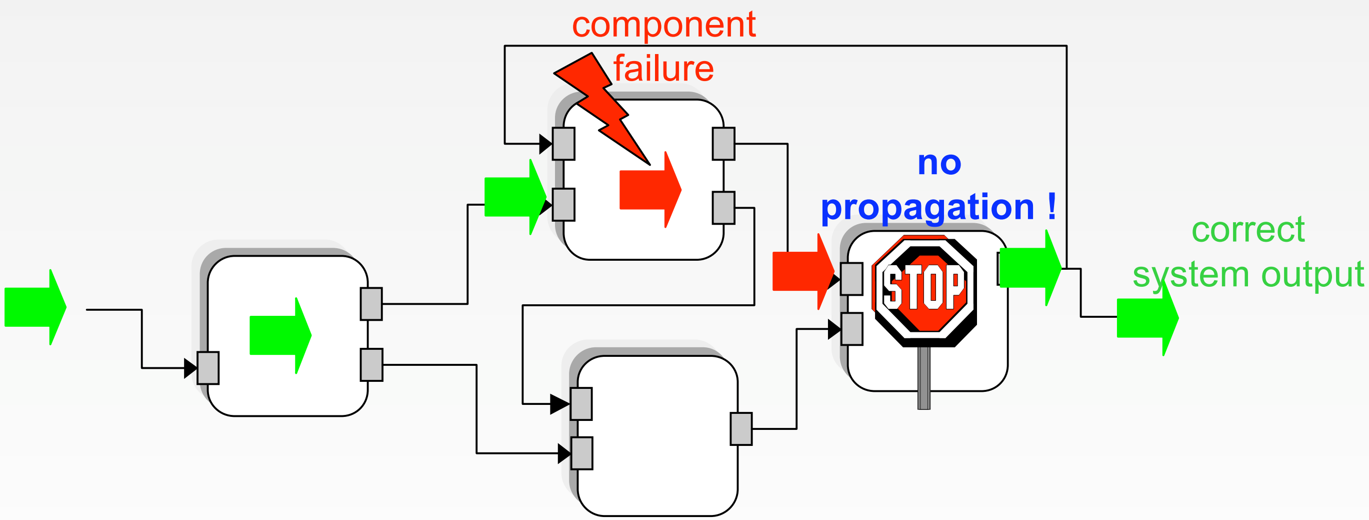
- ***Reliability***: *probability of successfully completing a given system task*
- Component failures may affect this probability
- How?



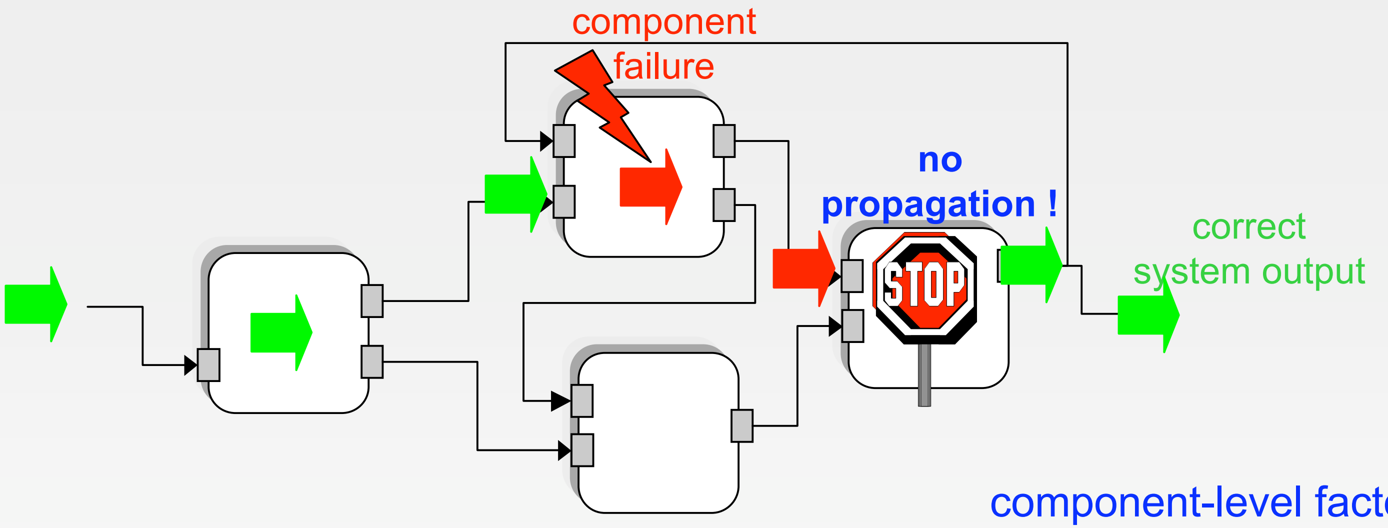
- a fault in a component causes an error in that component (erroneous state)
- an error manifests itself as a component failure (deviation from intended behavior)
- a component failure leads to a sytem failure if it “reaches” the system interface

Error propagation in component-based systems

- A component failure does not necessarily cause a system failure
  - subsequent components may not *propagate* the error



Factors affecting the system reliability



component-level factors

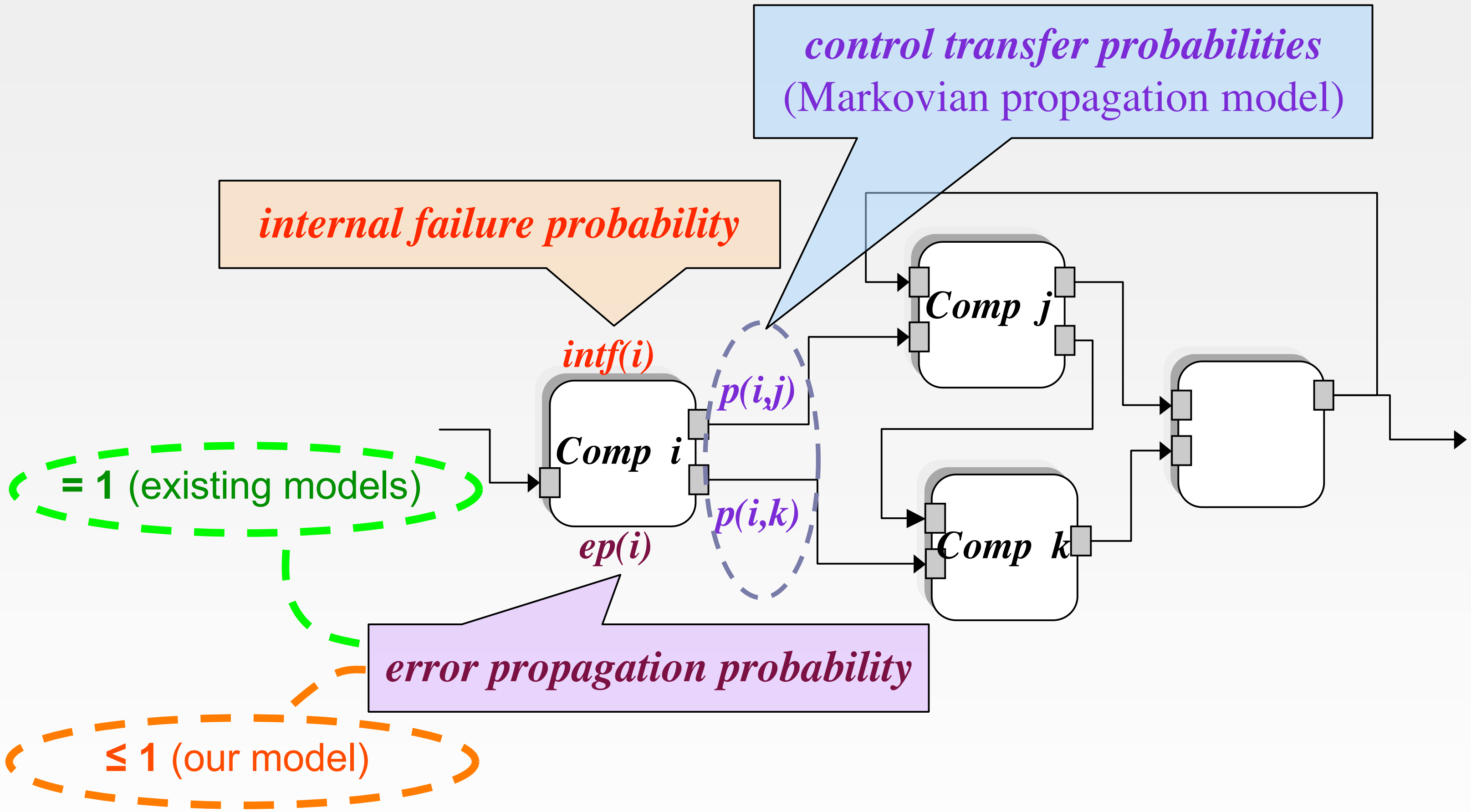
- Failure probability of each component
- Error propagation probability of each component

architecture-level factor

- Propagation path probability through different components

- (to the best of our knowledge) all existing reliability analytic models assume that a component failure **always** causes a system failure
  - ➡ error propagation probability = 1

Probabilistic model of a component-based system



- neglecting the impact of error masking/propagation may lead to overly pessimistic analysis results
  - risk of unncessary design and implementation efforts to improve reliability
  - risk of wrong decisions in component and architecture selection

Just a taste of our mathematics … :-)

$err^{(k)}(i,j)$: probability that the application reaches comp. *j* after *k* control transfers, starting from comp. *i*, and *j* produces an erroneous output

$$err^{(k)}(i,j) = p^{(k)}(i,j) \cdot intf(j) + ep(j) \cdot (1 - intf(j)) \sum_{h=0}^{C} err^{(k-1)}(i,h)\, p(h,j)$$

$\mathbf{e}$: vector of the probabilities that the application (for each possible initial component) produces an erroneous output

$$\mathbf{e} = (\mathbf{I} - \mathbf{Q})^{-1} \cdot \mathbf{F} \cdot (\mathbf{I} - \mathbf{Q} \cdot \mathbf{R} \cdot ((\mathbf{I} - \mathbf{F}))^{-1} \cdot \mathbf{c}$$

Our result

- based on this probabilistic model we …

- ... derive a **closed-form matrix expression for reliability evaluation**

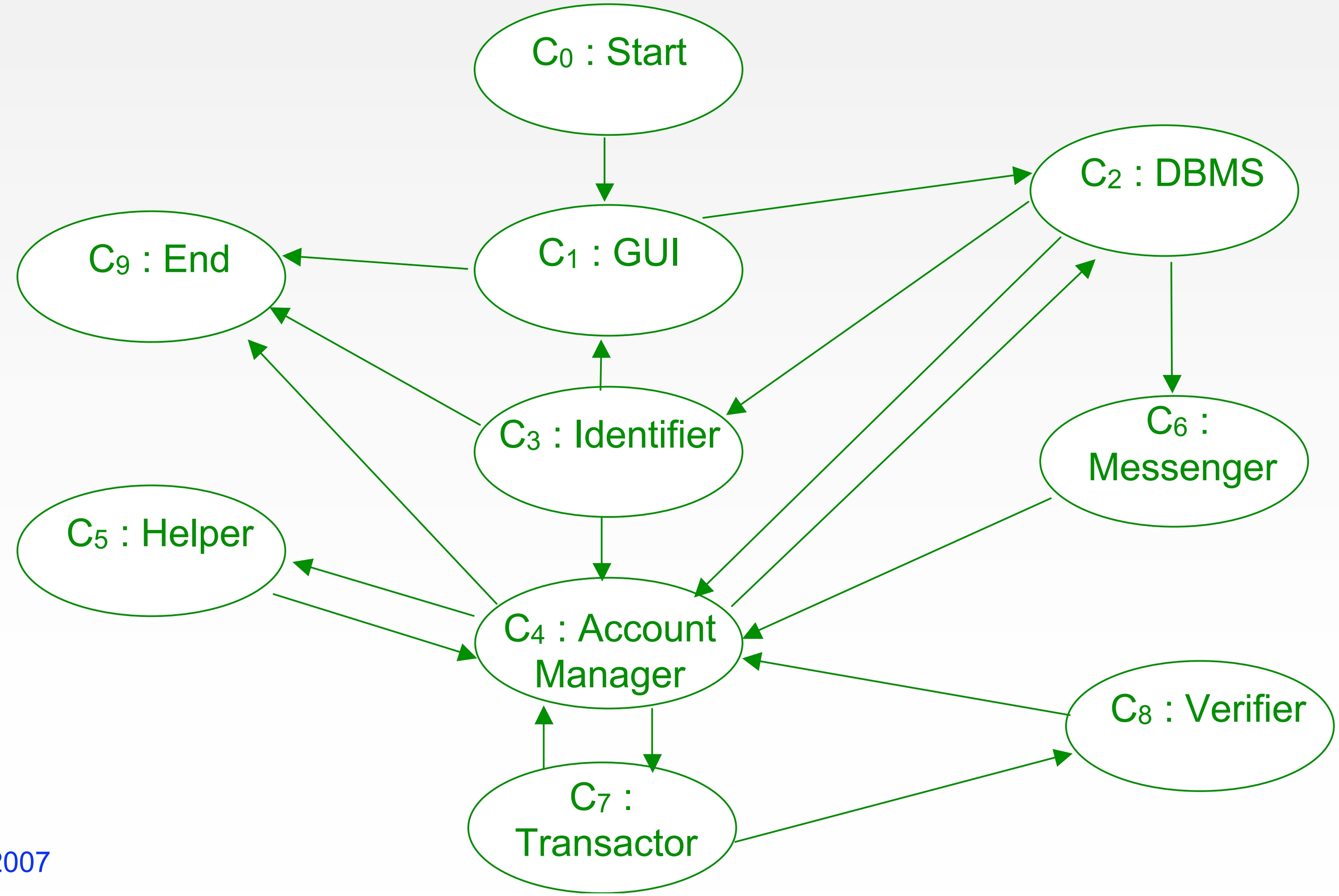
- … derive a **closed-form matrix expression for sensitivity evaluation** of reliability with respect to :
  - failure probability of a component
  - error propagation probability of a component

- … in both cases taking into account the error propagation

  - more realistic reliability prediction of a C-B system

Example : an ATM system

- 8 components : C1, C2, … C8 (C0 and C9 are fictitious components)
  - see paper for values of model parameters : *intf*(*i*), *ep*(*i*), p(*i*, *j*)   *i*, *j* = 0, 1, 2 … 9
    - (taken from : W.-L. Wang, D. Pan, M.-H. Chen, Architecture-based software reliability modeling, *Journal of Systems and Software*, no. 79, 2006, pp. 132-146)



Example : impact of error propagation on system reliability

- two alternative components : C4.1   C4.2
  - which one should be selected?

ignoring error propagation (that is, assuming *ep*(4.1) = *ep*(4.2) = 1) :

- C4.1 with *intf*(4.1) = 0.004 ➡ system reliability = **0.4745**

- C4.2 with *intf*(4.2) = 0.008 ➡ system reliability = **0.4594**

the system with C4.1 is slightly better

considering error propagation :

- C4.1 with *intf*(4.1) = 0.004 and *ep*(4.1) = 1 ➡ system reliability = **0.4745**

- C4.2 with *intf*(4.2) = 0.008 and *ep*(4.2) = 0.9 ➡ system reliability = **0.7094**

the system with C4.2 is largely better !!

Example : sensitivity to error propagation (1)

	C1	C2	C3	C4	C5	C6	C7	C8
$\dfrac{\partial Rel}{\partial ep(i)}$	-0.0199	-1.7830	-0.4360	-4.2732	-0.4246	-0.2001	-1.6031	-1.5853

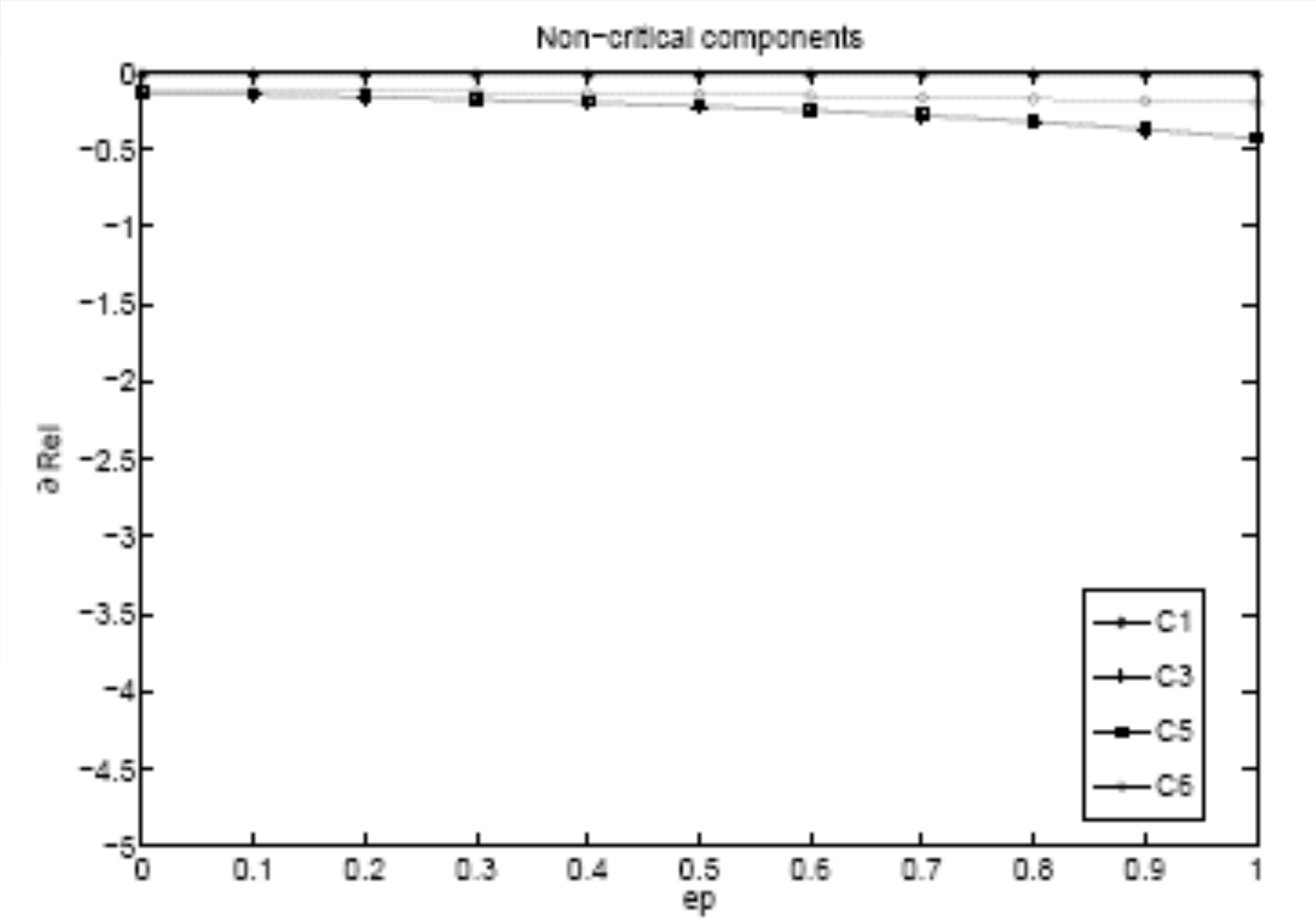
evaluated at
ep(*i*) = 1

critical components (C2, C4, C7, C8)

- similar results also with respect to *intf*(*i*)

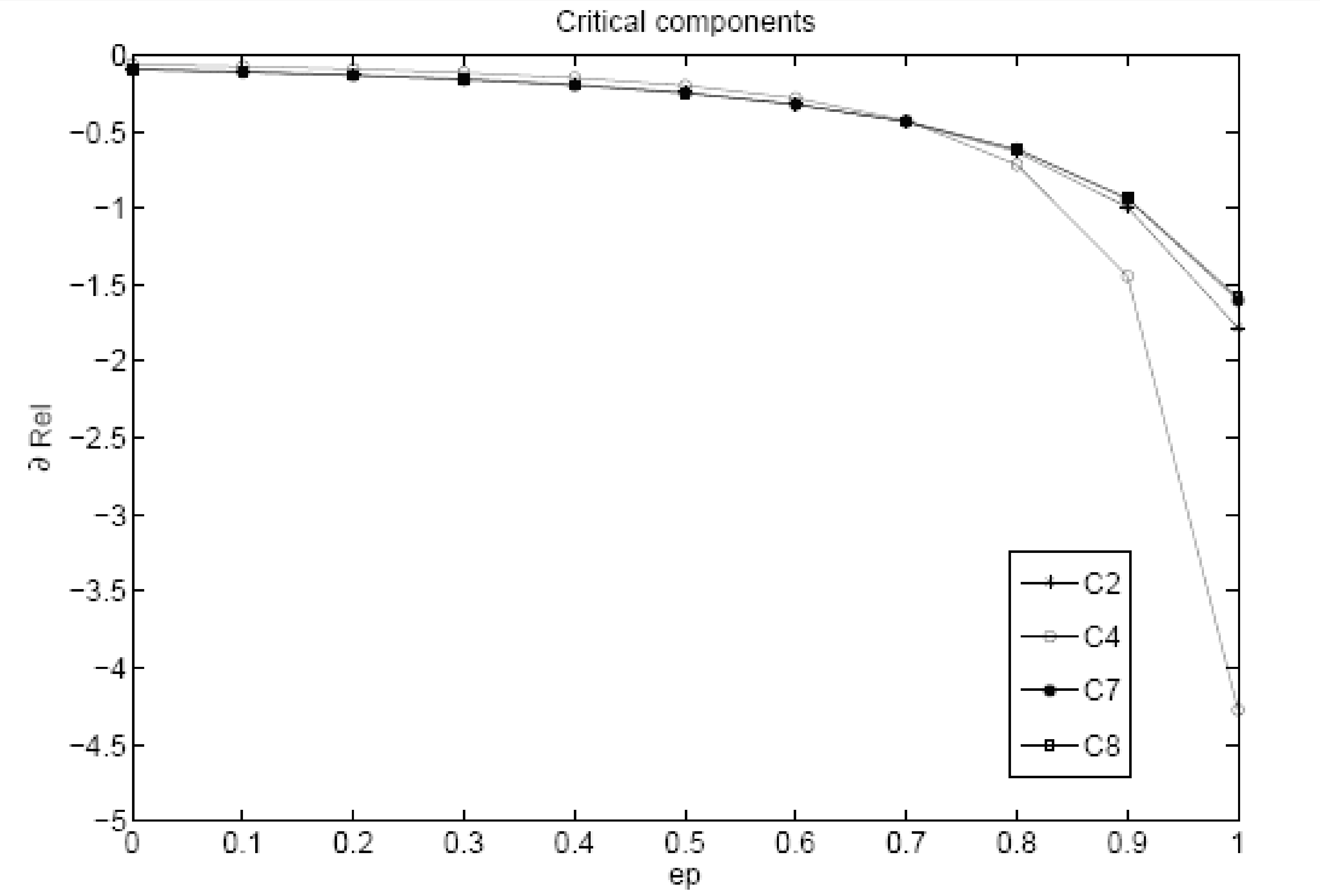
Example : sensitivity to error propagation (2)

- non-critical components :



Example : sensitivity to error propagation (3)

- critical components :



Some issues … (1)

- parameter estimation
  - *internal failure* and *control transfer probabilities* :

    we share the problem with most of the existing analytic reliability models of C-B systems (see K. Goseva-Popstoianova *et al.* (2001), S. Gokhale *et al.* (2004))
  - *error propagation probability* :

    see approaches by : M. Hiller *et al.* (2004), A. Mili *et al.* (2004)
- architectural issues
  - connectors?
  - underlying platform?

    … we are working about that
    - (see V. Grassi, in LNCS 3549, *Architecting Dependable Systems III* , 2005)

Some issues … (2)

- Control/propagation pattern
  - the Markovian model implies a sequential pattern
  - other patterns (e.g. parallel, …) ?

    they could be considered at least partly in the model using lumping techniques

    – (see W.L. Wang *et al.* (2006), V. Grassi (2005))

Some issues … (3) (from reviewers' suggestions)

- refining the propagation model : ➔ error prop. probability depending on both source and target component
  - easily included in our model: ***ep*(*h,j*)** instead of ***ep*(*j*)**

$$err^{(k)}(i,j) = p^{(k)}(i,j)\cdot intf(j)$$

$$+\, \xcancel{ep(j)}\cdot(1-intf(j))\sum_{h=0}^{C} err^{(k-1)}(i,h)\,p(h,j)\,ep(h,j)$$

- refining the component/failure model : ➔ different offered services may have different failure and/or propagation probabilities
  - easily included in our model: in all parameters ***intf*(*i*), *ep*(*i*), *p*(*i,j*),** substitute ***i j*** with i_h j_k, (where i_h is the *h*-th service offered by component ***i***)
  - (similarly to model different failure modes)

Some issues … (3) (cont.)

easily included

but ...

- increased model complexity, and ...
- (more important) more parameters to be estimated !!!

need of balancing accuracy with tractability/effectiveness

Some issues … (4) (from reviewers' suggestions)

- Error propagation
  - our model assumes propagation only among explicitly connected components
  - other kinds of side effects? ➡ open problem

Conclusions

- An analytic model which includes the error propagation/masking phenomenon
  - neglecting it may lead to misleading results
- Formal sensitivity analysis
  - identification of critical components
- Ongoing work ...
  - several issues that deserve further investigation