A Study on Multiformalism Modeling of Critical Infrastructures

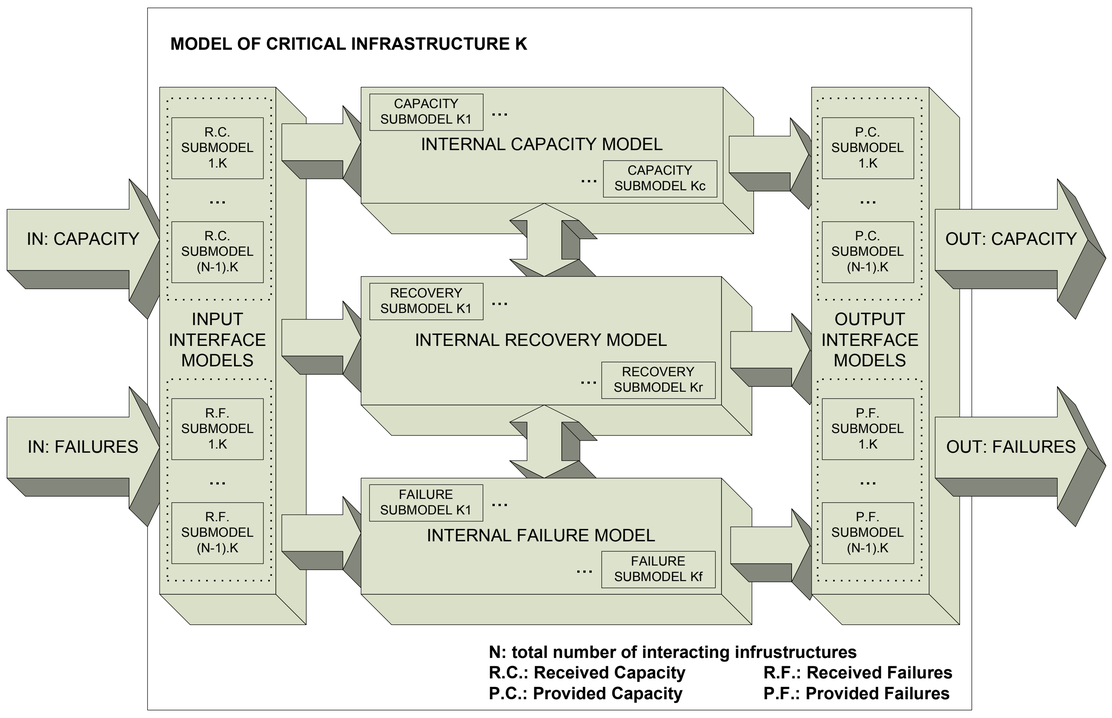
Francesco Flammini, Nicola Mazzocca, Concetta Pragliola, Valeria Vittorini

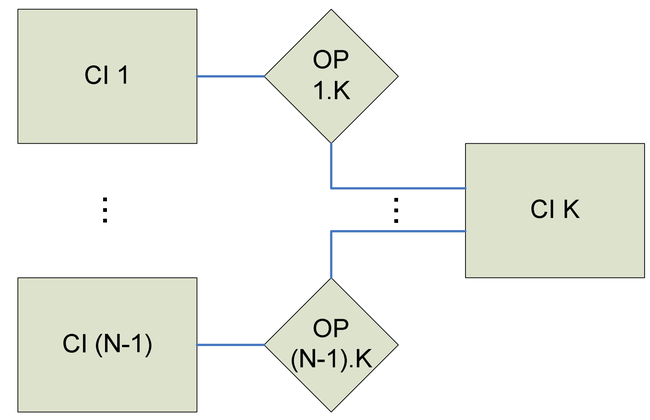
Rationale

Several frameworks have been proposed in the research literature in order to cope with critical infrastructure modeling issues, and almost all rely on simulation techniques. However, simulation does not allow to:
• analytically evaluate quantitative dependability attributes (such as Mean Time Between Hazardous Events, Vulnerability, Mean Down Time, etc.);
• verify properties on the model (e.g. the possibility to reach an unsafe state, the possibility that two specified infrastructures are unavailable at the same time, etc.).
These objectives can only be achieved using analytical approaches. Among these, multiformalism approaches allow modelers to adapt the choice of formal languages to the nature, complexity and abstraction layer of the subsystems to be modeled. Another advantage is the possibility of reusing existing (and validated) dependability models and solvers. Complexity and heterogeneity can be managed through modularity, and composition allows for representing structural or functional dependencies.

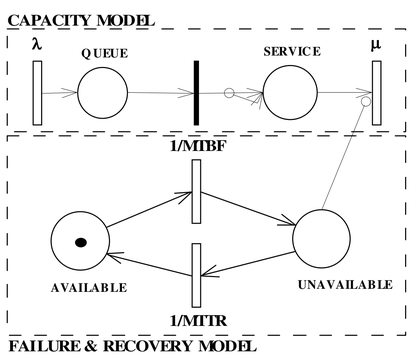
Objectives of the work:
• To explore the possibility of using multiformalism techniques for critical infrastructure modeling
• To propose a general scheme for intra and inter infrastructure models

General schemes for intra (left) and inter (right) infrastructure models

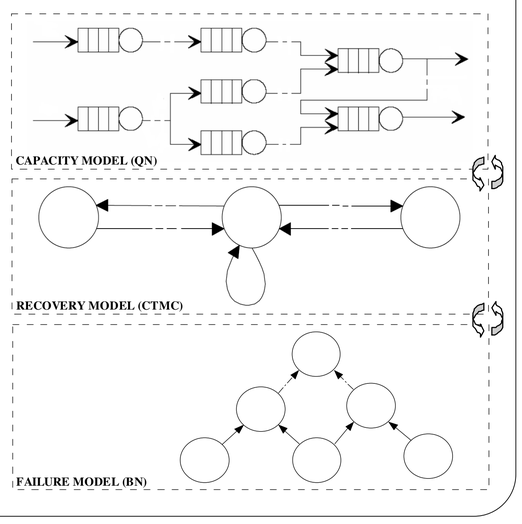




Basic models



Classic Generalized Stochastic Petri Nets (GSPN) performability model.



Inter-model connections:
• BN→CTMC: effect of failures on the infrastructure operating modes
• CTMC→QN: effect of the operating mode on infrastructure capacity
• QN→CTMC: infrastructure overstress
• CTMC→BN: imperfect recovery and overstress

Conclusions and future works

Conclusions:

- Multiformalism approaches well fit multilevel hierarchical modeling paradigms [2].

Future works:

- Complete case-study application of the methodology.
- Analysis and implementation of new composition operators [3].

Points requiring further analyses:

- The use of existing models could be limited by infrastructure operators for confidentiality reasons. To overcome this, models can be run in a distributed simulation environment only exposing their public interface, and the exchange of information to make them interact can be managed by the workflow engine in the OsMoSys modeling framework [1].
- Model-checking of multi-formalism models.

[1] Di Lorenzo, G., Flammini, F., Iacono, M., Marrone, S., Moscato, F., Vittorini, V.: The software architecture of the OsMoSys multisolution framework. In: Proc. 2nd Intl. Conf. on Perf. Evaluation Meth. & Tools, VALUETOOLS'07, pp. 1-10 (2007)

[2] Ezell, B., Farr, J., Wiese, I.: Infrastructure Risk Analysis Model. Journal of Infrastructure Systems, Vol. 6, No. 3, pp. 114-117 (2000)

[3] Gössler, G., Sifakis, J.: Composition for Component-Based Modeling. In proceedings of FMCO'02, November 5-8, Leiden, the Nederlands (2002)