SAFETY AND RELIABILITY ANALYSIS OF PROTECTION SYSTEMS FOR POWER SYSTEMS

Luca Ferrarini *, Leonardo Ambrosi * and Emanuele Ciapessoni **

** Politecnico di Milano, P.za L. da Vinci 32, 20133 Milan, Italy*
*** CESI RICERCA, Via Rubattino 54, 20134 Milan, Italy*

Abstract: This paper addresses the problem of risk analysis of protection systems and protection scheme of transmission grid. According to IEC 61508, a hybrid model has been developed supporting the analysis of protection systems. The use of analytic models in risk analysis of the elements of system protection scheme allows evaluating the security level associated to different protection strategies and supports the identification of specific ICT criticalities. *Copyright © 2006 IFAC*

Keywords: power systems, simulation, safety, standards, object-modelling technique, hybrid systems

1. INTRODUCTION

Like many other industrial and production systems, the field of production and transmission of energy is facing a trend towards deregulation, in Italy as well as in many European countries. This basically amounts to move from a single-operator, clearly regulated, easily predictable system to a competitive, uncertain, multi-operator system. The introduction of competitive supply and the organizational separation imposed by deregulation has resulted in highly stressed operating conditions and more vulnerable networks. Extremely important in this scenario is the definition of “quality” criteria, to be obeyed by market operators and vendors, in order to be able to positively cooperate to provide a correct service.

Strangely enough, in a market-oriented energy production and management, the “classic” deterministic criteria, adopted and useful in the regulated market, are still adopted to guarantee the security of the system. These are based on the fact that each abnormal operating condition contained in a suitable “contingency set” satisfies predefined performance criteria.

This allows to pragmatically design protection systems without considering all combinations of system configurations and operating conditions, which would be simply unfeasible. The deterministic approach, and the associated simulation methods, provides a simple rule to make decisions: optimize economy within the constraints of the secure operational region. This simplicity has made the deterministic method very attractive and useful in the past. Though effective in practice, the deterministic approach tends to focus on the most severe and credible event, thus producing an oversized and a less agile protection system, which reduces marginal gains and return of investments. Among others, the main deficiencies consist in not taking into account the frequency and the impact of events, and thus the likelihood of unwanted or catastrophic events, and in the negligence of non-limiting events.

This classical approach can be superseded by probabilistic risk based approach: several studies (Dobson, 2004b), (Lucarella et al., 2004), (McCalley and Vittal, 2001) demonstrated the possible gain associated to the use of risk based approach in the analysis and management of electric system security. Accordingly a CIGRE report (Marceau and Endrenyi, 1997) recommended to study probabilistic security assessment methods, and the CIGRE task force 38.02.21 is working on this recommendation. The Electric Power Research Institute (EPRI) was also involved in efforts to develop probabilistic risk assessment methods and tools for risk based security assessment (McCalley and Vittal, 2001). Following the risk-based perspective in the reliability analysis, the international standard IEC 61508 is the main normative reference. However, power systems exhibit a special behavior with respect to the safety and reliability problems, so that the standard needs to be integrated.

In this paper we pursue this approach by advocating the application of risk analysis techniques in the life cycle of protection system and protection scheme of the transmission grid. In particular, the goal is here to obtain a quantitative model in order to evaluate and compare protection systems and protection strategies able to improve the overall reliability of a system. Yu and Singh (Yu and Singh, 2004) followed this approach trying to define a simulation-based method to quantitatively evaluate hybrid stochastic models of power systems. That model was based on stationary continuous models (the so called "load flow model"), and discrete part is a logic model of the operating modes of a suitable combination of more physical components. The work here discussed extends that approach in these facts:

- instead only stationary continuous models, dynamic models are used (DAEs)
- a full modular approach has been adopted, implemented into an object-oriented hybrid dynamic simulator (Modelica/Dymola): any model of the system can be rewritten with more or with less detail without changing anything else of the system , provided that its physical interface is not changed of course;
- the discrete parts have been greatly improved, by separating components
- each discrete model of the physical component has a higher number of states, associated to physical phenomena and not to modes of operation.

The paper first summarize the relevant features of the power systems (Sect. 2) and then discusses the construction of the modular hybrid model in Sect. 3. Sect. 4 hints to the implementation into the simulation environment chosen.

2. CHARACTERISTICS OF POWER SYSTEM

2.1 Interconnections of subsystems

The substantial peculiarity of power systems consists in its complexity, wide area nature and strong interconnection of different subsystems. The system itself is composed of a high number of components belonging to a few types (*lines*, *bars*, *transformers*, *breakers*), but all these elements are electrically interconnected with variable topologies from zone to zone and country to country. This makes that anomalous behaviours of some components have unexpected consequences on others, which are located far away and which operate also in different conditions (Bie And Wang, 2001). Moreover the electrical connection makes the propagation of faults extremely fast.

Under these conditions, the risk assessment of the transmission system becomes a complex matter. While in fact the components are standard, their specific way of working while interconnected in real operating conditions are much more difficult and more uncertain to estimate in design phase.

Therefore, the concept itself of Safety Integrity Level (SIL) defined in the IEC 61508 standard must be revised, being insufficient if applied to single components, and being useless if applied to the entire system.

2.2 Undesired trips

The IEC 61508 basically focuses on the fact that protection systems may fail to intervene when a fault occurs in the system. On the contrary, one of the major causes of outages is constituted by undesired trips, often leading to cascade tripping. These are characterized by the fact that the protection system actually does intervene when it is not requested to do so, which constitutes a possible cause of cascading outages (Bie And Wang, 2001). Notice that the failure does not derive from a specific fault of a device, but from "external" factors to the protection, like the impossibility to measure the real current operating state (Padke, 2002), (Yu and Singh, 2004).

In order to consider these facts, it is necessary to define a common usage of reliability terms. We will use the *dependability* as the main property of a protection system. It concerns the ability to work properly and it is defined as the combination of *reliability*, the ability of a protection system to trip for a fault inside the protection zone, and *security*, the ability to refrain from tripping for fault outside the protection zone.

2.3 Dynamic constraints

This is one of the most important aspects of power systems, aspect that is ignored completely in the IEC standards. It consists in the fact that in many cases those limits that some process variables must satisfy to be in a "safe" condition can vary dynamically in time. This means that a system condition can be estimated as "safe" or not according to other operating conditions of the whole system.

Clearly, it is necessary to take this behaviour into account, both in the design phase of the protection systems and in its evaluation. In any case, it is necessary to develop models somehow adapt to the operating condition of the system.

This allows carrying out a much finer "dynamical" analysis than the classic static analysis of the system, which in turn allows to develop a definitely more precise protection system, on the base of specific risk-based indices of the transmission grid (Makarov, and Hardiman, 2003).

3. A HYBRID MODULAR MODEL FOR TRANSMISSION SYSTEM

One way to evaluate quantitatively the functional safety of the power system is the development of a model capable to capture both continuous dynamics of the system, its probabilistic nature, and its event-driven phenomena.

To this purpose, a suitable modular hybrid model (continuous and discrete event based), sketched in Fig. 1, has been developed. In that figure, the main elements (*lines*, *bars*, *transformers*, *breakers*) of the transmission grid are shown, with their own interfaces and connections.

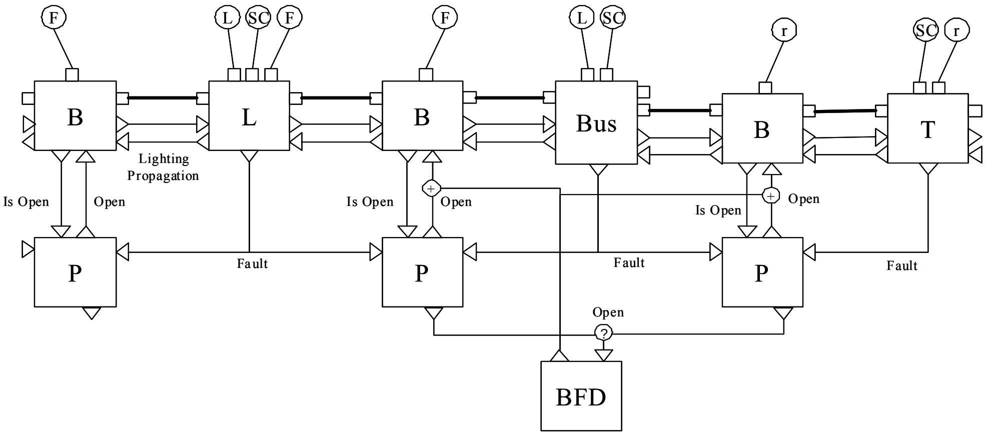

Fig. 1. Sketch of the hybrid model of the transmission systems

As it can be seen in the Fig. 1, each component has some connection with the neighbor. The connections painted with a thick line and a square interface represent the physical connections, i.e. the electrical connections regulated by the classical electrical equations. The connections painted with a thin line and a rectangular interface represent the logical connections, i.e. the way the discrete part of the model "inform" the others about their internal states, dispatching events.

Each module is internally described in a dual way, it has a discrete model and a continuous model that are able to communicate together as we'll see later.

The basic modeling criteria are the following.

- Modularity

It is advisable to have a component-wise modeling and simulation environment, where the user instantiates modules that directly correspond to physical components, instead of writing equations. This means that each module should be thought as the generic behavior of a component under generic constraints; the overall model will come out of the assembly of the basic components, and the user should not intervene in the assembling of equations.

- Hybrid behavior

It's necessary, since the system under investigation shows continuous-time behavior for electrical phenomena, and event-based behavior for discontinuous phenomena like breaks and faults (clearly enough, the modeling of "fast" phenomena as discontinuous is a modeling simplification, if one does not need to go into the atomic details of electricity transmission).

To do so, we implemented the discrete part of a model with Petri net, a well-known formal technique to represent discrete-event systems. Ordinary Petri net models have been extended, with a simple semantic rule, in order to generate outputs and receiving inputs with the continuous part.

The continuous part of the model is quite simply, each element is represented with the classics electrical components (impedance, inductance, switch, and so on), electrically connected with the continuous part of the other models.

- Discrete-Continuous connection.

Some of the transitions of the Petri net model have been endowed with a time delay, stochastically distributed as proposed in the GSPN formalism (Ajmone et al. 1995). This means that a stochastic transition is associated with a value representing the mean time to fire, once enabled, generally represented with the symbol λ_i.

Notice that some of those λ_i are exogenous (i.e. represent physical phenomena that have external causes with respect to the model itself, like the falling of a tree or thunder on the system), but other are not. A typical example relates to the cascade effect. Consider for example the rate of failures of an electrical component. This depends on the instantaneous current circulating in it, as hinted in Fig. 2.

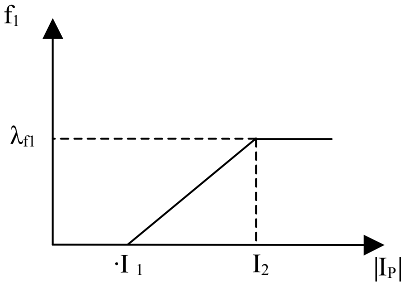

Fig. 2. Fault rate dependence from the circulating current (an example) for an electric device

From the modeling and simulation point of view, this means that the fault rate of a (stochastic) transition of the Petri net model of the discrete-event part of the model of a component depends on the value computed in the continuous time part of the model of the same component. Here clearly arise the connection between the discrete and the continuous part of the model.

This is clearly not a trivial step, since again the continuous part depends on the discrete one, and since the occurrence of future events can not be pre-calculated since other events may occur in the meanwhile.

In fact, if an electrical part should break, the circulating currents and the voltage calculated by the continuous part should change, possibly influencing again in the future the discrete part.

In the sequel, some details are provided on the modeling of the basic components of the power transmission system.

3.1 Line

The line is the basic transmission element for power. The continuous model takes into account the fact that a line can be interrupted (by a breaker or a fault), can be short-circuited (a fault, or an external cause, like a falling tree for example) or can be hit by thunders. The modelling of the lightning effect on lines has been simplified to a logic behaviour (a switch), being the physical modelling out of the scope of this project. Thus, the basic continuous behaviour is sketched in Fig. 3, where Z_{L1}, Z_{L2}, Z_{cc} are impedances.

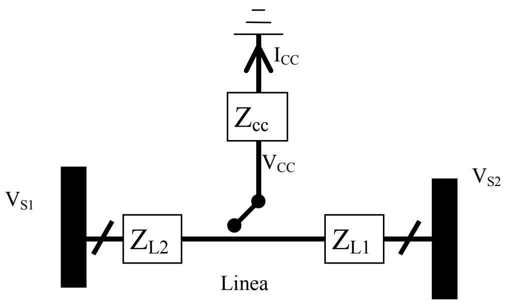

Fig 3.– Basic continuous behaviour of the line

The discrete time part describes all the other behaviour of the net (see Fig. 4).

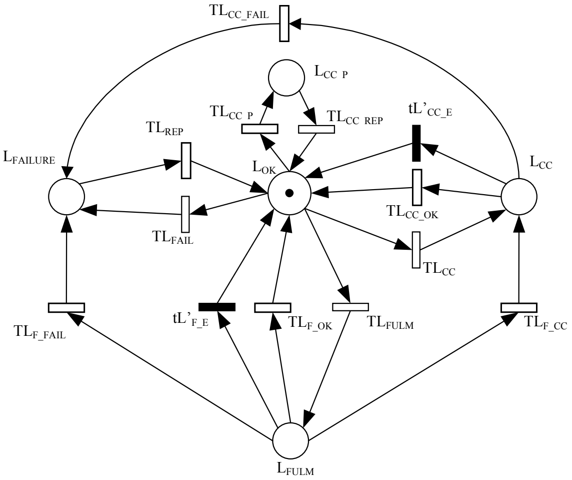

Fig. 4. Petri net model of a line

The meaning of the places and transitions is hinted in the following.

Places:

- L_{OK} = line is healthy.
- L_{CC} = line is short-circuited
- L_{CC_P} = line is permanently short-circuited
- L_{FULM} = line is lightened
- $L_{FAILURE}$ = line is faulty

Transitions:

- TL_{FULM} = the line is struck by a lightning
- TL_{F_OK} = the lightning is extinguished autonomously and the line returns in OK state. (L_{OK})
- tL'_{F_E} = the lightning is extinguished by the intervention of protections,. This immediate transition is conditioned by $|I_{LINE}|<\varepsilon$
- TL_{CC} = the line from the state of OK goes to short-circuit with ground
- TL_{CC_OK} = the short-circuit is autonomously extinguished
- tL'_{CC_E} = the short-circuit is extinguished by the intervention of protections. This transition is conditioned by $|V_{LINE}|<\varepsilon$

- TL_{CC_P} = the line goes from OK state to permanent short-circuit
- TL_{CC_REP} = line is repaired to eliminate the permanent short-circuit
- TL_{FAIL} = failure of a line (normally caused by an object)
- TL_{REP} = line is restored to OK state
- TL_{F_FAIL} = failure of a line caused by a lightning. The effect of the lightning is extinguished
- TL_{F_CC} = the line goes to short-circuit because of a lightning. The energy of the lightning is considered discharged to the ground.
- TL_{CC_FAIL} = the line fails because of a short-circuit (normally caused by the breaking of an insulator)

The overall behaviour of the Petri net model can now be deduced quite straightforwardly.

Finally, the interaction of the two sub-models. It is clear that, if the line change its internal state, the topological view of the net can change, and consequently the electrical calculus. Besides the change of the value of the electrical variables, make change the λ regulating the fire rate of the discrete transition. It is quite obvious, for example, that if an external event occurs, like a short-circuit caused by a falling tree, then the fictitious switch shunting the line to ground is closed and at the same time a transition in the Petri net part is enabled.

2.2 Breaker

The breaker has been modelled with a similar approach. It has four main logical states: open, close, stuck closed and stuck open. The transition from one state to another one are quite simple and be deduced with an easy spot of the name of the transition. The Petri net model is sketched in Fig. 5.

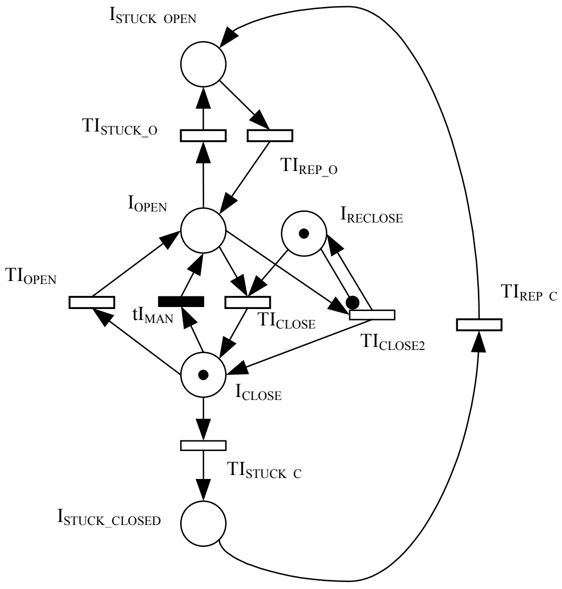

Fig. 5. Petri net model of a breaker.

As it can be argued, also the automatic re-close operation has been modelled. Actually, after an open operation, the breaker can be closed (modelled with a stochastic transition). Should the breaker be opened again, then it can be closed again only with transition Tclose2, only once: such a transition will be conditioned to the fact that the lines attached to it are in "functioning" state.

Transitions:
- tI_{MAN} = opening of the breaker triggered by manual command or by backup devices (Breaker Failure Device)
- TI_{OPEN} = opening of the breaker triggered by the associated protection
- TI_{CLOSE} = fast reclosure of the breaker
- TI'_{CLOSE2} = reclosure of the breaker conditioned by "OK state" of the connected elements
- TI_{STUCK_C} = failure of the breaker from closed to stuck close
- TI_{STUCK_O} = failure of the breaker from open to stuck open
- TI_{REP_O} = reparation of the breaker and restoration in state of stuck open
- TI_{REP_C} = time interval between the failure of the breaker and the moment in which the failure is recognized. The breaker is then opened and restored (TI_{REP_O} transition).

2.3 Bar and transformer

Similarly, also bars and transformers have been modelled. Details are here omitted for the sake of simplicity.

4. SIMULATION

In order to evaluate quantitatively the above model, a suitable simulation environment is to be used. The simulation engine should be accurate enough to deal with continuous-time dynamics, event-based dynamics, and stochastic behaviours. Our choice is the Modelica/Dymola environment. It's an object-oriented modelling and simulation framework, with an easy-to-comprehend component-oriented description, with different physical and communication ports, endowed with a fine symbolic manipulation of equations, which allows both the user to "describe" the equations directly in the continuous time domain and to obtain an optimised simulation code. It's a time-based simulator, which means that the discrete-event part must be suitably treated for efficient and effective implementation, and similarly there is no support for stochastic behaviour, which must then be explicitly introduced.

Currently, the basic models of line, bar, transformer, breaker, generator and load are under final testing.
Such specific and reusable components have been modelled as hybrid systems, whose internal behaviour is given by a suitable combination of continuous dynamic sub-module with a discrete-event stochastic sub-module.

In particular, to do so, the stochastic Petri net sub-module has been directly implemented in Modelica, exploiting the capability of using "external functions". Special care has been paid to the modelling of switching behaviours (due to e.g. breakers or faults) and to the mutual interaction between the continuous and the discrete part of each component, and the "transmission" of events between components.

The description of the modelling choices is matter of future works, along with the application to the IEEE Reliability Test System prepared by the Reliability Test System Task Force of the Application of Probability Methods to Power Systems.

5. CONCLUSION AND FUTURE WORK

The application of IEC 61508 to the life cycle of E/E/EP systems for the protection of transmission grid, depends on the identification of appropriate risk analysis techniques, able to manage the complexity and wide area nature of the grid, and supporting the identification of the required security level. To this aim, the paper proposes a hybrid model, based on Generalised Stochastic Petri Net integrated with continuous simulations approach, supporting the risk analysis and evaluation of different protection strategies, on the base of specific risk-based indices.

The paper describes the hybrid model, taking into account both the continuous time dynamics of the power system itself, but also the discrete dynamics involved by disrupt phenomena due to breaks, outages, natural phenomena.
The use of analytic models in SIL analysis of the element of system protection scheme allows to evaluate the security level associated to different protection strategies and to support the identification of specific criticalities of protection system.

Acknowledgement. This work has been supported by MAP (Italian Ministry for Productive Activities) in the frame of Public Interest Energy Research Project named "*Ricerca di Sistema*" (MAP Decree of 28 Feb. 2003).

REFERENCES

Ajmone, M.Marsam, G. Balbo, G. Conte, S. Donatelli and G. Franceschinis (1995). *Modelling with Generalized Stochastic Petri Nets*, Wiley Series in Parallel Computing, John Wiley and Sons.

Bie, Z., and X. Wang (2002). Evaluation of power system cascading outages. *IEEE Power System Technology Intl. Conference.*. **Vol. 1**, 13-17 Oct. 2002, p. 415 – 419.

Marceau, R.J., and J. Endrenyi (1997). "*Power System Security Assessment: A Position Paper*". CIGRE Task Force 38.03.12. Electra, **No. 175**, pp. 48-78.

Dobson, I., B. A. Carreras, V. E. Lynch and D. E. Newman (2004a). Complex Systems Analysis of Series of Blackouts: Cascading Failure, Criticality, and Self-organization; *Bulk Power System Dynamics and Control*, Cortina d'Ampezzo, Italy.

Dobson, I., B. A. Carreras and D. E. Newman (2004b). A criticality approach to monitoring cascading failure risk and failure propagation in transmission systems; "*Electricity transmission in deregulated markets" Conference at Carnegie Mellon university.*

Grigg, C. et al. (1999). The IEEE Reliability Test System-1996: a report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee Power Systems. *IEEE Transactions on Power Systems*, **Vol. 14**, Issue 3, pages 1010 – 1020.

Lucarella, D., M. Pozzi, M. Valisi and G. Vimercati (2004). Un approccio basato sull'analisi di rischio per l'esercizio in sicurezza del sistema elettrico; Italian National Congress on the estimation and management of risk in civil and industrial sites; Pisa, Italy.

Makarov, Y.V., and R.C. Hardiman (2003). On Risk-based Indices for Transmission Systems. *Proc. IEEE PES Annual Meeting*, Toronto, Ontario, Canada, July 13-17, 2003

McCalley, J. and V. Vittal (2001). Risk Based Security Assessment, EPRI Project WO8604-01, 2001, final report.

Padke, A. (2002). Hidden failures in protection systems. *Power systems and communications infrastructures for the future*, International conference, Beijing, 2002.

Yu, X., and C. Singh (2004). A Practical Approach for Integrated Power System Vulnerability Analysis With Protection Failures, *IEEE Transaction on power systems*, **vol. 19**, no. 4, pages 1811 – 1820.