Coordinador de la propuesta:
Bermúdez de Castro, Alfredo

Representante de la Empresa:
Izquierdo Rocha, José M.
Sánchez Perea, Miguel

TITULO DE LA ACTIVIDAD: JORNADAS DE CONSULTA MATEMÁTICA PARA EMPRESAS E INSTITUCIONES. i-MATH 2008-2011

Risk Assessment and Protection Engineering

A short view of a new discipline

The mathematical modeling and simulation department (MOSI) at CSN is responsible for setting-up and maintaining a computer simulation infrastructure, and an associated methodology, to help performing independent checks of industry safety assessments, both deterministic and probabilistic, of the Spanish nuclear power plants.

From these activities, the ones related to modeling the dynamics of accidents as part of the review of the plant protections, frame the type of problems and techniques for their solutions that may be worth to share with and consult the academy about. They also deserve more widespread attention because:

- the techniques developed by the nuclear industry to ensure safety and to protect the public and the environment, have potential to be most useful in many other domains with equivalent protection problems; those associated with the damage that the operation of large and complex systems may generate, from industrial complexes to financial institutions.
-this extension requires integration into a new discipline of the different aspects involved, with the goal of optimizing the design and operation of adequate protections. It maybe properly called Protection Theory, in parallel with Control Theory that is similarly devoted to optimize the control systems that automate the operation of the facilities in order to optimize their benefits.

Although control and protection engineering are parallel in their goals, and similar in its dynamic systems background, risk assessment techniques are essential in protection but not necessarily so in control, clearly indicating that we are talking about a closely related, yet different discipline. It may be considered a special branch of the system reliability world as much as one of the control engineering world, where the fault and event tree techniques

that are familiar to the reliability engineers combine with the strong flavor of system and process dynamics that is familiar to the control engineers.

Problem description.

For the purposes of this short note, we understand by Protection Engineering the discipline, methods and technologies that deal with the design and optimization of protective measures, both manual and automatic, in (usually large) industrial facilities. The optimization is constrained by acceptance criteria derived from general public risk limit regulations, as described for instance by risk limit curves.

Optimization is needed in order to assure intervention if necessary and prevent it if unnecessary; a requirement derived from the often-aggressive nature of the safety measures. Decision for interventions ought to be automatic in the short term after an accident and concurrently, and interactively manual, soon after. Time scales may vary from seconds to days or even months and very complicated phenomena may appear as a result of the interaction between the plant and the automatic systems. It paves the way for scenarios that easily escape individual's mind capability to predict behavior and requires carefully planned emergency instructions.

We denote generically as facility protection the set of systems, system features, and safety oriented decision-making processes whose objective is to optimize plant response with respect to damage under any credible event. Regulations and regulatory bodies should ensure that the facility protection prevents undue public risk should those events occur. Note the enveloping character of the analysis, which makes Protection Engineering assessment so complex and singular. Assessing damage for a few particular events is of little regulatory interest. What counts is to prove that under no credible circumstance can damage indicators go over unacceptable limits. These limits are inherently probabilistic in nature, since they are functions of the frequency.

Computer modeling, understood as the process to make precise statements and translate ideas into computer language, provides a rigorous framework for simulation to explicitly represent the impact of both protective measures and decisions for their interventions during the time evolution of accident scenarios. The results of the simulation and the defense of its underlying safety case allow for a traceable procedure for compliance with

damage exceedance frequency risk acceptance criteria. As a result, safety assessment may be viewed as a computer aided protection-engineering methodology based on simulation.

As of today, a substantial body of theory, in rapid evolution during the last decade, is providing a sound scientific basis as well as identifying improvement areas. In our department we have selected a particular approach based on the *stimulus driven theory of probabilistic dynamics* (SDTPD). Overall, the theory attacks the optimization of the protection of complex systems. The main figure of limit, extensively discussed throughout the nuclear and financial community, is the frequency of exceedance of a given damage. The SDTPD integrate damage due to accident scenarios with scenario frequency by formulating equations for the exceedance frequency.

Among many, we have selected two different aspects from which we are interested in specific mathematical problems where help from academy is welcome.

1. *Analysis of damage scenarios*.

Here, the key point is that damage indicators (generally algebraic functions of process variables) should be chosen and safety limits associated to them. Accident trajectories that violate those limits define unsafe states, a concept that parallels but is very different to unstable states in control. Their description leads to damage domains as the set of all possible damage trajectories.

The challenge is how to identify them. We have devised a (new??) specific approach by revisiting old and classical control techniques -based on one dimensional s-domain linear transfer functions to identify stable states- then extending them into piecewise linear systems, using finite (instead of classical) Laplace transforms and extending the transfer function approach into a multi s-domain transmission functions to identify unsafe states via new mathematical "chain" operators.

Transmission functions offer then an alternate view of mathematical modeling of dynamic systems appropriate for protection where advise from the scientific community will be welcome.

2.- Analysis of scenario frequencies and computation of the damage exceedance frequency.

Here the key point is how to incorporate reliability engineering and its contribution to assess the frequency of each scenario, a perspective that makes much different the protection problem from the control problem. Indeed, risk regulatory limits are set on the exceedance damage frequency so both frequency and damage are an intrinsic part of the formulation of the protection problem.

The stimulus driven theory of probabilistic dynamics, SDTPD, originally an application of the Chapman-Kolmogorov approach into continuous events on dynamic systems, seems to be equivalent to a piecewise discontinuous stochastic Markov process with transition rates strongly dependent on the dynamics, equivalence that allows a computer algorithm and a method that we call the TSD (theory of stimulated dynamics) risk assessment method. Again, to ensure this equivalence and to study the possibility for this formalism to be solved with the transmission function artillery (also in this second aspect), it will be helpful to have the academic opinion and knowledge. Additionally, the relationship between the present "implicitly dynamical" approach (classical probabilistic safety assessment, PSA) and the TSD method is of paramount interest.

If successful this proposal makes a practical transition from static to dynamic reliability that will improve the assessment and design of protection systems.

The two problems and their techniques will be presented as independent of any application field as possible, and diverse examples taken from different domains will be used as illustration.