UNDERSTANDING COMPLEX SYSTEMS INSTABILITIES TO PREVENT CRISIS OF CRITICAL INFRASTRUCTURES

Claudio Balducelli
ENEA[1]

Keywords

Systems instability, Critical Infrastructures, Inter-dependency, Cyber-vulnerabilities, Socio-technical systems

Abstract

"Instability" is a an undesired phenomena that occurs when a system responds to external stimuli in a way the makes it less controllable. An instable state of a system is a condition in which very low variations of the state parameters may produce a system behaviour that, in some cases, could also generate the system collapse.
From experiences and analyses, that will be illustrated in this work, is possible to discover that physical systems instabilities are today in most cases well known and can be better understood considering past accident scenarios.
But new type of instabilities, coming from the cyber and organisational layers must be well analysed in the next future. These researches have to address the problem of making risk and dependability analysis applicable not only to physical systems but also to socio-technical systems. More in particular this new type of risk analysis had to deal with the interdependencies problem typical of the "complex systems". It is necessary a better understanding about how some vulnerabilities or attacks inside the cyber and organisational layers of the critical infrastructures, could generate or amplify instabilities in the physical layer. At the same time is necessary to know how much stable a physical system must be for not collapsing in presence with new instabilities coming from cyber and organisational layers.

Introduction

Every type of physical system can work in a more o less stable working condition; to avoid the collapse is important to know what configuration of the state parameters generates an increasing or a reduction of the system stability level. In this paper the instabilities of the physical systems are analysed, considering different types of plants and infrastructures for which non only the physical layer but also the cyber and organisational parts could be critical.
In the nuclear reactor field, boiling water reactors cores are considered instable when they work at low power and low water flow: the phenomena of high mode power oscillations in the core is illustrated as one of the principal effect of instability of these type of reactors. A specific scenario including regional power oscillations was observed in october 1993 during the special tests conducted by ENEA-AMN at Caorso nuclear power station to test core instability level of this plant. This type of physical instability is described in section 1.

[1] ENEA - Italian Agency for New Technologies, Energy and Environment
Via Anguillarese 301, 00060 Rome, Italy
e-mail: claudio.balducelli @casaccia.enea.it

For an electrical transmission network the frequency, the voltage profiles and their associated stability margins are considered and analysed; their deviation from normal state could made the network more instable and vulnerable. The specific emergency scenarios occurred during the Italy-Swiss black-out, happened on September 2003, the black-outs in Canada-United States on August 2003 and the last event in Germany in November 2006 were also determined by some intrinsic instability of the networks that was augmented by human and organisational errors. The importance of the available recovery time during the crisis is also considered; the time available for recovery actions depends on the degree of network instability, and it could allow the execution of emergency operator procedures. The main factors that that make more instable the energy transmission network are analysed in section 2.

Some lessons learned about the causes and the conditions that generate systems instability are elicited from the previous specific cases and from other similar cases, occurred in the past.

Starting from common considerations about these instability cases, some general features that characterise the systems instabilities are evidenced and illustrated in section 3 as potentially applicable to every type of systems or networks.

When we consider Critical Infrastructures, we have to take in account that they are not simply physical plants but contains also a cyber and an organisational layer including the information/control system components and the human organisations supporting and controlling the normal operation of the whole infrastructures.

Cyber and organisational layer supervise and control the physical layer, and must first of all take under control the potential instabilities of the physical system. The globalisation of the markets generates computer based system, technical solutions and human organisations more instable now than in the past. These new aspects of the system instability problem are analysed also in section 3

Finally, in section 4 some key recommendations are indicated to try to mitigate the Critical Infrastructures instabilities.

Physical instabilities: lessons learned from nuclear power plants

The local power generation in the core of a nuclear reactor is directly related to the neutron flux, which itself is a function of the reactivity. In BWRs, the reactivity depends strongly on the core void fraction. Thus when a void fraction oscillation is established in a BWR, the power oscillates according to the neutronic feedback. This feedback mechanism which is shown in Figure 1 in a simplified manner may under certain conditions lead to poorly damped or even limit-cycle *power oscillations*.

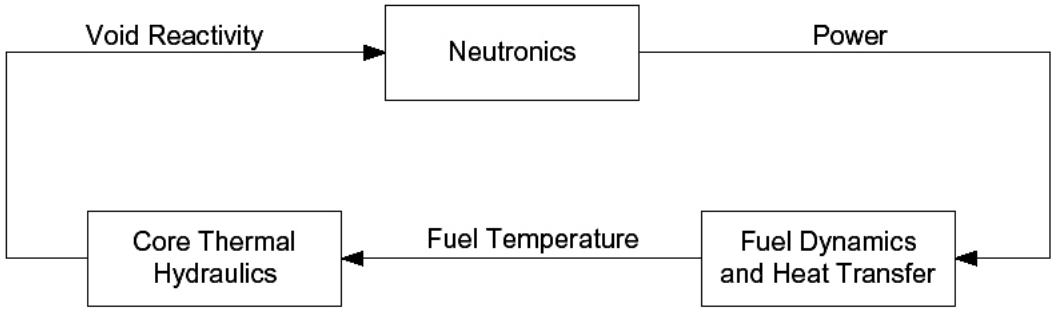

Fig 1 – Feedback mechanism of the void reactivity

Their frequency lies around 0.5 Hz, that is about twice the transport time of the coolant through the core (T = 1/0.5 = 2 sec). Amplitudes from nearly 0% to more than 100% in power have been observed. The oscillations, in different parts of the reactor core, are mostly global, i.e. they are "in-phase".

Higher mode power oscillations are also possible; these divide the core into two regions oscillating in opposite directions at constant overall power. These regional oscillations are cumbersome for the operators since their detection is not directly possible with standard instruments that display only core-average data. Even more complex modes of instability have also been observed.

During the early years of BWR technology, there was considerable concern about the possible effect of coupled neutronic/thermal-hydraulic instabilities. However, after various in depth experiments and analyses, it became clear that BWRs could be designed such that instabilities would not occur under normal operating conditions. In fact the normal reactor operating point, characterised by the Core flow and the Thermal power, is *far from the operating conditions in which instabilities may occur*. This situation is visible in fig 2 in which it is recognised that instability of the reactor core may happen only in operating points where Core Flow is less than 50% and Thermal Power less than 70% and more then 35%.

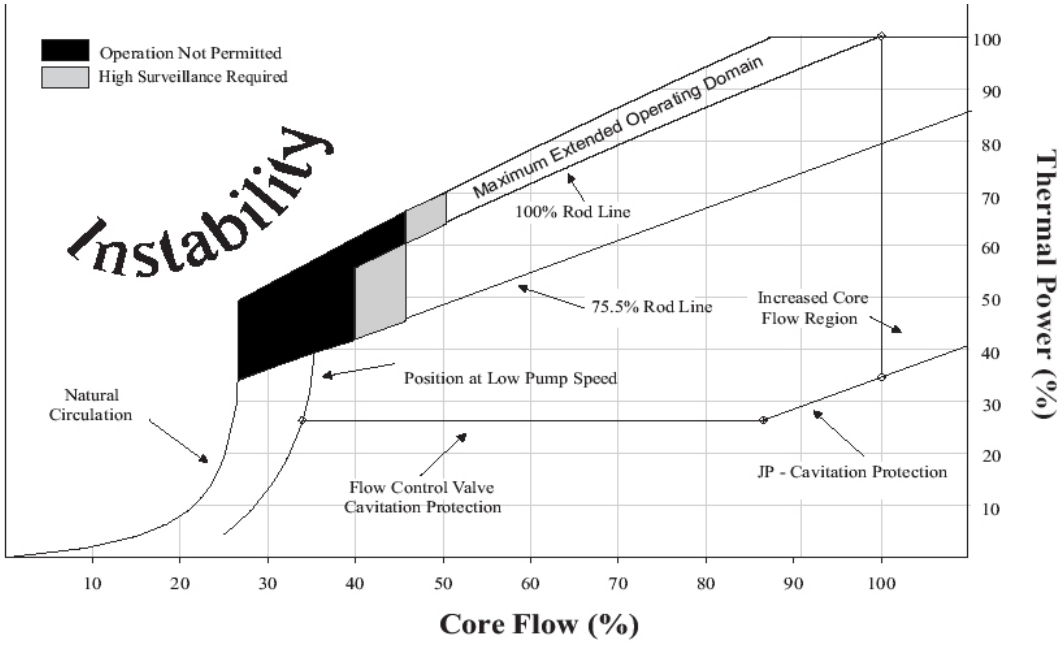

Fig. 2 – Operative map of a Boiling Water reactor core

Several nuclear reactor plants experienced power-void oscillations, during special tests, similar to the test conducted by AMN-ENEA on Caorso Power Plant the first of october 1983 in which the instability regions was reached under operative controlled procedures. From these experiences the nuclear reactor operators recognised the possibility to arrive, in safe conditions, near the instability points.

Lesson learned from this experiences was that, to have a more complete control of the plant, is necessary to know in advance in what part of the reactor core map (Core Flow versus Thermal Power) the instability phenomena occur. This knowledge may be acquired with special controlled tests and also with system simulation analysis (Ginestar D. *et al*, 2002). In other words is necessary to know not only what may be the "normal" working condition of

the physical system, but also what are the working conditions to be avoided for preventing instability phenomena.

Critical Infrastructures instability

In the last years it was recognized that Critical Infrastructures (Rinaldi S.M *et al*, 2001), suffer of major instability problem today respect to the past.

This problem has today a greater impact on the emergency management community, and its significance has increased since governments and citizens became aware that services furnished by power distribution networks, telecommunication networks, transport infrastructures and other key resources are actually more critical than in the past. To maintain their style of living, modern societies are more dependent on their critical infrastructures; but, ironically, critical infrastructures seem to be less stable than in the past. Some new types of vulnerabilities are candidates to having a strong impact in the future emergency management practices and social security strategies.

The need for protecting critical infrastructures becomes more important also as a consequence of the so-called 'cascading effect', caused by the mutual 'interdependencies' (Rinaldi S.M, 2001), of the networks. There are different causes and external conditions that contribute to augmenting such type of interdependency. When we consider critical infrastructures, we have to take into account that they are not simply 'physical' plants and networks. In fact, they contain not only a physical layer, but are also made of 'cyber' components and systems, and include human organisations to manage and supervise the daily operations of the infrastructure.

Anyway if we look only at physical layer, as the example of fig 3 for an electricity network, it is possible to discover a lot of similarity of their potential instability with the instability of the nuclear reactor core described in the previous section.

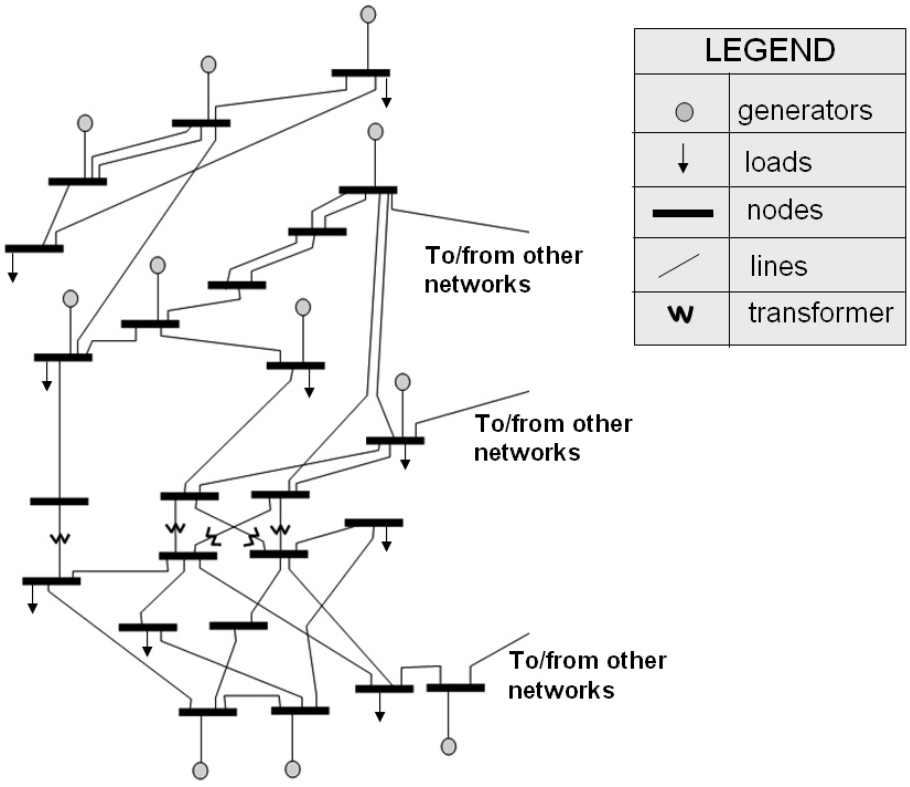

Fig. 3 – A simple electrical transport network

In fig. 3 is shown a simple electrical transport network, as it is described in the IEEE Transaction paper (1999). The basic elements in the network are:

- the "generators", that are different types of power production plants (Oil/Steam, Coal/Steam, Hydro, Nuclear etc.) and represent the points in which energy is produced,
- the "loads" that represent the points in which power is consumed (by a city distribution network, by an industry or by a railway energy substation),
- the "nodes" that represent the buses where generators and loads are connected,
- the "lines" that represent the electrical cables in which power flow from the generators to the loads or toward other networks, as the foreign network.

Different portions of the network generally work at different voltage levels, and are interfaced with "transformers".

The stable working condition of such system may be explained in the same way as could be explained the stability of a tandem bike on which more cyclists are pedalling (Soder L., 2002).

Every cyclists have to pedal at the same frequency since all sprockets are connected with same chain. Also in the electrical network all the generators (turbines) have to rotate at the same frequency to maintain constant (50 hertz) the electrical power frequency.

If some cyclists are simply sitting on the bike and do not pedal they could be compared to the loads of the electrical network; in fact they are points in which the energy produced by the other cyclists is consumed. To keep constant the speed of the bike the total force of the active cyclists (total generation) has to be the same as the total power absorbed by the passive cyclists (total loads). It could be noted that the chain between the cyclists may be slightly elastic; it means that an angle difference may exist between the pedals positions of the different cyclists. The same phenomena happens in the electrical network when a "phase angle" exists between active and reactive generated power, and all the generators have to work in such way to reduce as much as possible these phase angles differences. For the bike system a great angle difference indicates that some cyclist pedal too slowly and some other too fast. In the electrical transmission network the angle difference indicates also an insufficient power production in some part of the network and a surplus of production in some other parts. In such situation, for the bike and for the network system as well, some instability conditions could arise.

It interesting to note that, in the previous condition, the instability level of the tandem bike system increases much if the bike speed is low (bike oscillations can arise), and, on the contrary, decreases when the speed of the bike increases.

In the same way, also the electrical network system results more vulnerable, due to such instability problem, when the electrical production and consumption is low. The Italian electrical black-out of September 2003, mainly determined by a too high energy flow from foreign countries, happened during the night, the period in which the energy production and consumption are low; the Italian energy operator (GRTN) said in such occasion that the same black out may be avoided during the day, when production and consumption are higher.

If we look again at the nuclear core operative map of fig 2, we could note that, also for this system, the instability condition is higher when the core flow is low (30-35% of the nominal flow).

From the above considerations we can learn the following lesson: to work in a safe condition, whatever the considered system is, the system operator have to maintain its parameters near the nominal working states. System shutdowns or start-up must be executed with attention, because during the execution of such procedures may be possible to pass through zones where the system instability is higher, and a collapse event may occurs.

Causes that determine the physical instability of the networks

The globalisation of the markets makes more difficult for the networks operators to manage the systems in a safe working status, far from the instability zones.

Generally the electrical system operator of a certain nation have to decides or plans the day before what generators (production plants) will be used the day after to satisfy the internal energy consumption and the external requests. This is imposed by the fact that it is not possible to execute rapid start-ups or shut-downs of the production plants. Depending on the plant typologies these procedures may require long times (hours) for the execution.

In the energy field new possibilities were recently introduced for distributed generation of renewable energy like solar energy or wind. But the power transmission networks and their control and supervisory systems are not ready to manage these new autonomous energy producers that introduce additional instability inside the electrical system. In fact is not always possible to forecast with sufficient accuracy where and when the weather conditions requested by the renewable energy production plants will be available. This types of plants have a "degree of autonomy" that is not always compatible with the need to maintain the whole system in a safe condition (far from the instability zones).

The consequence of the serious incident, which originated in the North German electrical grid during the night of 6 November 2006, was simply the European grid separation in three large islands, but, on this occasion, Europe risked a very large blackout, involving a lot of countries. One of the reasons of this incident was also attributed to voltage instabilities caused by the wind energy production plants, installed in the North of Germany by autonomous energy providers.

The free energy market imposes today also the necessity to sell and acquire energy from different countries during some time periods that are determined by economical reasons, but that do not take in account the systems instability constraints.

One of the main reasons of the electrical network instability, which in September 2003 generated the collapse of the Italian grid, came from the large amount of energy imported by Italy from France. The cost of this energy is lower if transferred in the night period. This determines a higher amount of power flow coming from France to Italy during the night. But in such condition, when fewer generators are in operation, the total voltage stability margin is narrow, and the network has less degrees of freedom to manage potential instabilities caused by the high cross-border power flow.

Cyber and organisational instabilities

When we speak about Critical Infrastructure instabilities we have consider not only the faults arising in the physical layer of the infrastructure but also what happens on the cyber and the organisational layer (Balducelli C. *et al*, 2005).

This situation is well described in the table of fig 4, extracted from the Joint United States-Canada Power Outage Task Force report, that shows the sequences of events happened on august 14 2003, four hours before the collapse of the US-Canada power grid.

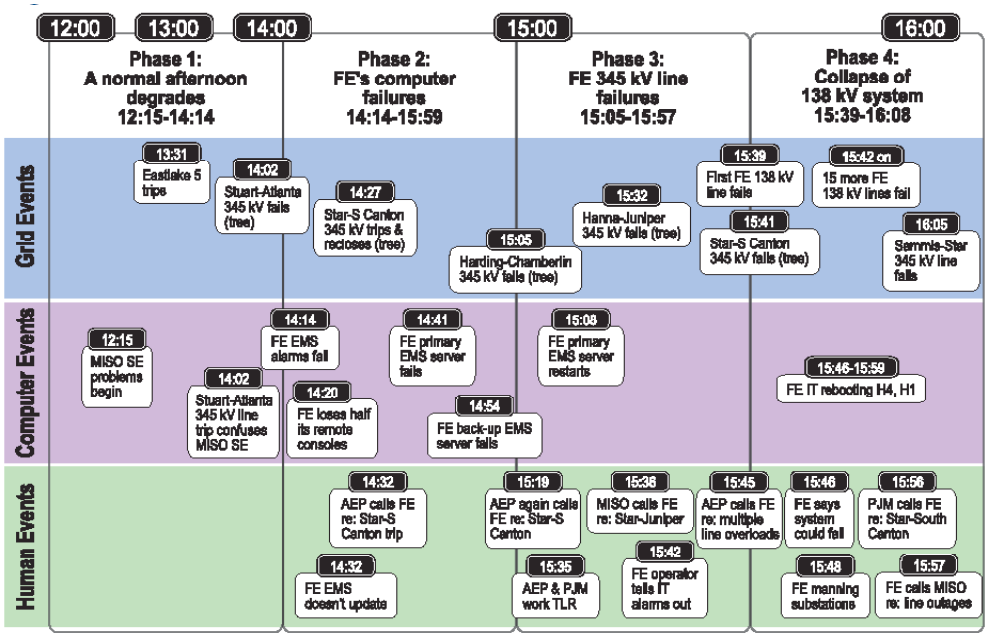

Fig 4 - Timeline of the U.S- Canada Power System outage

In the table the events are classified as physical (grid) events, computer (cyber faults) event and human events (operator errors), and at every event the relative time label is associated.

From the figure is possible to evidence that in this case the first events of the chain was caused by some computer faults: the program MISO SE (the State Estimator tool) utilised by the electrical operators to evaluate the status (stability level) of the physical network gave some wrong indications. For such reason after 12:15 the electrical operators were not completely aware about the real state of the network.

They were not alerted about some instabilities that started inside the network; without the proper corrections, the instability levels increased, and many other physical faults arose like several lines disconnections. As it is visible in the bottom part of the figure, also many wrong types of operations ware executed as the operators didn't understand the causes of the alarms that arrived in certain sequences at control rooms.

This situation describes well as a cyber infrastructure, that is designed to allow the operators to maintain the physical network far from well known instability zones, contains some intrinsic vulnerabilities that may cause itself some not foreseen instabilities.

Other vulnerability points of the cyber infrastructure depend on the cyber-attack possibilities that increased in the last years. Some time cyber attackers may exploit also the same automation mechanisms designed to increase the cyber-infrastructure efficiency.

New instabilities appeared also in the human organisations managing infrastructures. In the global world this is generated by the necessity to reduce the organisational and industrial costs, that for a company are determined by the competition with other companies.

The globalisation of the markets and the competition make both computer systems and human organisations more vulnerable and exposed to external threats.

Sources of instabilities in the cyber layers are also caused by loss of employers or industry operators with critical skills. The introduction of a new generation of information/control systems often requires more knowledge/expertise about these new technologies. But

frequently, the companies are afraid about the introduction of new technologies, and at the same time, the oldest ones are not competitive anymore.

To reduce personnel cost, many energy distribution companies promote the utilisation of 'remote' maintenance of devices and cyber components utilising the internet connectivity. But this new type of connectivity can be used also by malicious users or cyber-terrorists to damage the network functionality.

Some key recommendations to reduce complex systems instability

The physical layer of the system have some "intra-dependency" with the software components dedicated to monitoring and controlling the internal functions. For the most important and critical infrastructures these components belong to a cyber layer that is called SCADA[2] system.

Regarding SCADA system many misconceptions exist, and, in particular one of these is the idea that "SCADA system resides on a physically separate, standalone network". In effect most SCADA systems were originally built before and often separate from other corporate networks. As a result, IT managers typically operate on the assumption that these systems cannot be accessed through corporate networks or from remote access points. Unfortunately, this belief is usually fallacious. In reality, SCADA networks and corporate IT systems are often bridged as a result of two key changes in information management practices. First, the demand for remote access computing has encouraged many utilities to establish connections to the SCADA system that enable SCADA engineers to monitor and control the system from points on the corporate network. Second, many utilities have added connections between corporate networks and SCADA networks in order to allow corporate decision makers to obtain instant access to critical data about the status of their operational systems. Often, these connections are implemented without a full understanding of the corresponding security risks. In fact, the security strategy for utility corporate network infrastructures rarely accounts for the fact that access to these systems might allow unauthorized access and control of SCADA systems.

For these reasons SCADA systems have been protected as their internal failure, eventually caused by attacks, may contribute to produce physical instability phenomena.

Another important issue that may be considered to reduce the physical systems instabilities is the need of *more coordination* between the different organisations managing critical networks and infrastructures.

It is well known that inside every infrastructure many procedures, tools and resources are available for the operators to prevent and manage crisis or instability events. Anyway every infrastructure operator normally looks inside his own infrastructure and has the primary goal to protect it against failures and disruptions. Anyway actually the infrastructures are more and more interconnected; they produce services and materials that are utilised by other infrastructures; the lack of a certain service inside a local infrastructure may produce failure inside remote one that, if consequently fails, could produce additional damage inside the local one. This is the so called "interdependency" phenomena (Rinaldi S.M, et al, 2001) that, for more coupled infrastructures, seem to be a new and emerging instability problem.

While for the instability problems encountered inside single plants, the local operators are generally trained to maintain the system inside the operative zones, far from well known

[2] Supervisory Control And Data Acquisition system

instability regions, interdependency is a new instability phenomena, affecting sets of coupled infrastructure, for which the operators have not sufficient information and knowledge.

To front this new type of instability is necessary to co-operate and to exchange information between different infrastructure owners about the status of critical services that are essential for the survival of some other coupled infrastructure.

In this type of communication there are two main types of information that have to be exchanged to mitigate the possible instabilities arising from interdependency problems:

Info about quality of services

The infrastructure that acts as service provider informs the service consumer about the quality of the service delivery. Information can not only be related to actual service delivery but also to "future service delivery". Information related to future service delivery may be accompanied with a probability of occurrence. One purpose is that the service provider can inform the service consumer of possible future problems to give the service consumer sufficient time to take mitigation measures. In the case of incidents, it might be important for the service consumer to know that the problems are not within its own infrastructure but are related to a failure of a consumed service.

Negotiation info

In this case the service provider and the service consumer negotiate the terms of possible service degradations. One party sends a proposal to the other one. Proposals contain suggestions concerning the minimum quality of service levels for certain services, time spans and locations. The other partner can then accept or reject each proposal. Negotiation messages are always exchanged in both ways. There are different possibilities how negotiation can start. For example, an electricity distributor has to disconnect a certain area for some time but he is flexible with the exact time. He can suggest possible times for the disconnection and a telecommunication provider can choose one of the options. Another possibility is that a service consumer sends, as a reaction to an information about quality of certain services for the next future, a preference list with the most important services. These preferences can be considered during recovery crisis and recovery phases.

Conclusions

We described how instabilities are a sort of intrinsic phenomena for every types physical systems. Every complex systems like energy plants, energy distribution or telecommunication networks have some cyber and operational layers dedicated to monitor and control the system instabilities.

Actually complex networked systems are the core of many critical infrastructures, that are coupled together and that exchange critical services each other. Instabilities of a specific physical system are often well known by the systems operators and they have sufficient knowledge to avoid intra-system cascading failures.

But, when the interdependency problem between more infrastructures arises, the operators are not sufficiently prepared and a not usual co-ordination strategy is needed.

EU IRRIIS integrated project (IRRIIS, 2006), started one year ago, with the objective to produce a set of software components (based on MIT – Middleware Improved Technology) to be installed as mutual co-ordination support for the different infrastructures operators. We hope that the results of this project will be available as soon as possible to address and solve, almost in part, the increasing instability of critical infrastructures.

References

Ginestar D., Miro R., Verdu G., Hennig D., (2002). Transient Modal Analysis of a BWR instability event, Journal of Nuclear Science & Technology, Vol 49, No. 5, 554-563, May 2002.

Rinaldi S.M., Peerenboom J.P., Kelly T.K., (2001). Identify Understanding and Analysing Critical Infrastructures Interdependencies, IEEE Control System Magazine, p.p. 11-25, Dec. 2001

"The IEEE Reliability Test System – 1996" (1999), IEEE Transaction on Power Systems, Vol. 14, No. 3, August 1999.

Soder L. (2002). "Explaining Power System Operation to Nonengineers", IEEE Power Engineering Review, April 2002, p.p 25-27

Balducelli C., Bologna S., Di Pietro A., Vicoli G., (2005). "Analysing Interdependencies of Critical Infrastructures Using Agent Discrete Event Simulation", Proceedings of 12th TIEMS Conference, May 24-27 2005 Faroe Islands.

IRRIIS (Integrated Risk Reduction for Information-based Infrastructure Systems) (2006), EU IP Project, **www.irriis.org**

Author Biography

Claudio Balducelli is a senior scientist working at ENEA as project manager since 1983 in the field of AI technologies applied to operator decision support systems for emergency industrial accidents. His interests include operator models, knowledge formalization, planning, computerized procedures, plant diagnosis, case based reasoning, learning and fuzzy algorithms. He co-ordinated also the prototypical implementation of various site applications like a cooperative training system for the Genoa Oil Port managers (MUSTER project) and an emergency operator support system for major Oil Deposits and Pipelines in Italy. He is team leader inside SAFEGUARD FP5 project (Safeguarding Critical Infrastructures), and IRRIIS (Integrated Risk Reduction of Information-based Infrastructure Systems) FP6 project.