EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre

Electric System vulnerabilities: a state of the art of defense technologies

Alberto Stefanini and Marcelo Masera

ipSc

Institute for the Protection and Security of the Citizen

2006

EUR 21890 EN

EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre

Electric System vulnerabilities: a state of the art of defense technologies

Alberto Stefanini[*] *and Marcelo Masera*

Institute for the Protection and Security of the Citizen

[*] Alberto Stefanini is currently working at the Institute for Protection and Security of the Citizen of the Joint Research Centre as a National Detached Expert from CESI - Milan

Mission

The mission of the Institute of the Protection and Security of the Citizen of the Joint Research Centre is to provide research-based, system-oriented support to EU policies so as to protect the citizen. The main application areas are cyber-security and the fight against fraud; natural, technological and economic risks; humanitarian security, non-proliferation and nuclear safeguards. The Institute will continue to maintain and develop its expertise in information, communication, space and engineering technologies in support of its mission.

LEGAL NOTICE

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which may be made of the following information.

Acknowledgement

The authors would like to thank Angelo Invernizzi and Massimo Pozzi, CESI, Prof. Nick Kiriakopoulos, Univ. of Washington, and Prof. Nouredine Hadjsaid, LEG-INSIEG Grenoble, for the many insights and the advice given on early drafts of this report.

EUR 21890 EN

Printed in Italy

Abbreviations

CIGRE’: International Council on Large Electric Systems

ICT: Information and Communication Technologies

ISO: Independent System Operator

SCADA: Supervisory Control And Data Acquisition

TSO: Transmission System Operator

UCTE: the Union for Coordination of Electricity Transport

Executive Summary

Vulnerability of the European electrical infrastructure appears to be growing due to several factors:

- demand is always growing, and, although this growth may be forecast, it cannot be anytime easily faced;
- transactions increase, following electrical system liberalisation, and this involves operating the whole infrastructure closer to the system capacity and security limits;
- an increased control systems complexity, required for secure system operation, may in turn raise system vulnerability, due both to accidental faults and malicious attacks;
- critical infrastructures, and the electrical system primarily, are well known to be a privileged target in warfare, as well as terrorist attacks.

In recent years, both Europe and America have experienced a significant number of huge blackouts, whose frequency and impact looks progressively growing. These events had common roots in the fact that current risk assessment *methodologies* and current system *controls* [1] appear to be no longer adequate. Beyond the growing complexity of the electrical system as a whole, two main reasons can be listed:

- system analysis procedures based on these *methodologies* did not identify security threats emerging from failures of critical physical components;
- on-line *controls* were not able to avoid system collapse.

This report provides a state-of-the-art of the technology on both regards:

- as far as risk assessment *methodologies* are concerned, an overview of the conceptual power system reliability framework is provided, and the current N-1 principle for risk assessment in power systems is introduced, together with off-the-shelf enforcement methodologies, like optimal power flow. Emerging methodologies for dynamic security assessment are also discussed. The power system reliability approach is compared with the global approach to dependability introduced by computer scientists, and the conceptual clashes pointed out. Ways ahead to conciliate both views are outlined.

- concerning power system *controls*, the report overviews the existing defense plans, making specific reference to the current Italian situation. The two major recent blackout events in the American North East and Italy are analysed, and the drawbacks of the existing arrangements and the installed control systems are discussed. Emerging technologies, such as phasor measurement units and wide area protection are introduced. Their likely impact on the existing control room is discussed. Finally, potential cyber vulnerabilities of the new control systems are introduced, the role of communication standards in that context is discussed, and an overview of the current state of the art is presented.

[1] by power system *controls* we mean here both the procedures for system management, and the related information and communication infrastructure, comprehensive of monitoring, actuation and protection devices.

1 Introduction

1.1. What happened in the Summer of 2003?

Summer 2003 was characterised by electricity supply disruption events which had wide impact on a number of key economies; these events contributed to direct attention on how crucially modern societies depend on correct operation of the electric power infrastructure. They also evidenced to what extent all technological infrastructures depend on electricity supply. On the other hand most interdependencies are not usually perceived not only by the public at large, but also by most infrastructure operators; hence they are not taken into appropriate account into the relevant contingency planning.

In the current context, threats against the electrical system are growing – like for other network-shaped, highly distributed infrastructures – due to two concurrent factors:

- demand is always growing, and, although this growth may be forecast, it cannot be anytime easily faced (also because the public often contrasts construction of new power generating plants and transmission lines) [UCTE, 2004b, UCTE, 2004c]. Power systems have been developed in the past 50 years so as to ensure mutual assistance between national subsystems including common use of reserve capacities and, to some extent, to optimise the use of energy resources by allowing exchanges between these systems. Today's market development with its high level of cross-border exchanges was out of the scope of the original system design. Transactions increase, following electrical system liberalisation, and this involves operating the whole infrastructure closer to security limits, see Section 2.1 [Eurelectric, 2004];
- market liberalisation involves that multiple operators exchange critical information so as to jointly operate the system, hence a number of key control systems need drastic reviews in order to fit to operation in a market context. The electrical system depends substantially and increasingly from its supporting information and communication infrastructure, because almost all system vital functions are remotely controlled, so that an increased control systems complexity, required for secure system operation, may in turn raise system vulnerability, due both to accidental faults and malicious attacks. Critical infrastructures, and the electrical system primarily, are well known to be a privileged target in warfare, as well as terrorist attacks. Unless appropriate measures are taken, this risk will increase with the adoption of open and public information and communication infrastructures for automation support.

These risk factors are increasing with progressive establishment of a European energy market: .the summer 2003 blackouts are likely to be the first ones where inadequacy of the system *controls* was the key factor:

August 14, 2003 – American North East

The event was triggered by a contact between a tree and a 345 kV line (these contacts are rather usual and their likelihood increases with power flow due to line sagging). *The event was in a way induced and, above all, inappropriately managed because of some impending problems affecting the monitoring and control equipment.* Indeed, the *state estimator* used to get a picture of the current system state, was out of order for approximately 4 hours and was restarted a few minutes before the black-out (both due to human errors and to technical problems). Another fault to the SCADA server put the alarm management system out of operation and slowed down the entire SCADA functionality, affecting online data update in particular, hence making control room operators quite totally blind in front of the event [US-Canada, 2004].

August 28, 2003 – UK, South London

A combination of events led to an electricity power supply failure in south London that occurred at 18.20 on 28 August. Following an alarm caused by low oil level in a shunt reactor, a transformer was disconnected from the distribution system, as the normal practice in this case. Unexpectedly, automatic protection equipment interpreted the change of power flows, due to the transformer disconnection, as a fault, and disconnected 410,000 customers, including parts of London Underground and Network Rail system. Power supply was recovered in half an hour (though the restoration of underground operation took longer for safety reasons). *The cause of the incident was the incorrect rating of a protection relay, undiscovered by the extensive quality control and commissioning procedures* [National Grid, 2003] .

September, 23 2003 - Southern Sweden and Eastern Denmark

At 12.36 on Tuesday 23 September 2003 Eastern Denmark and Southern Sweden experienced a comprehensive blackout. The power failure was primarily caused by a fault at a substation in Southern Sweden. During a situation with a number of interconnections and power lines in maintenance and four nuclear units out of operation, the electric system in Southern Sweden experienced the loss of a large nuclear unit. Approximately 5’ after a double bus-bar fault in a substation on the West coast disconnected four out of five 400 kV transmission lines. Increasing flows on the remaining lines and low voltage in Southern Sweden made protection relays to trip. Consequently Southern Sweden and Eastern Denmark were completely disconnected from the Central after 90 seconds. *The root cause of the incident was the combination of the initial loss of the large nuclear unit with the double bus-bar fault in the substation on the West coast, which drove the system beyond its security criteria (N-3 situation)* [Elkraft, 2003].

September 28, 2003 – Italy

The degradation of the Italian system and the causes of its long restoration are mostly due to either inadequate or inappropriate behaviour of protection equipment. All three categories of protection systems (critical section control, load relief equipment, load rejection equipment) failed for different reasons [AEEG, 2004]. It is also remarkable that 21 out of 52 power plants failed to compensate the lack of imported power, because most of them rejected load at about 49 hertz, well above the stated threshold of 47.5 hertz [*ibidem*]. The inappropriate, overcautious setting was likely due to power plant operators' inclination to protect their assets from under-frequency operation.

Key issues

In summary, neither electrical system management nor operating procedures, nor system automation were revised so as to adequately cope with the liberalisation scenario:

- regarding the Italian case, the UCTE report [2004] points out as an accident originated in Switzerland did require the timely intervention by the Italian operator to be adequately dealt with. However the Italian operator does not have direct visibility on the events that happened in other countries, and therefore had to be warned on the phone from the Swiss operator;
- the American system alike lacks a governing body who may effectively coordinate operators activities. Although NERC, the US coordinating body, did advance a proposal to that effect [NERC, 1997], this met the opposition of several regional operators. Moreover malfunction of a critical software equipment (the *state estimator*), which were designed to act as a common reference for the operators, was a key factor after the triggering event, <u>in that it deceived operators on the likely progression of the electrical situation and its criticality;</u>
- in the Italian case, restoration was further compounded by *critical infrastructure interdependency*. After two hours, the emergency supply to several vital information and communication equipment ceased to work, hence this equipment could no longer operate. This required to resort to a backup satellite facility for communication, and to manually operate all the remotely controlled equipment, thus making restoration far longer and more cumbersome [AEEG, 2004];
- in the American case, restoration was even longer and more cumbersome, due to the inherent complexity and the extension of the crisis, the plethora of actors involved, and inadequacies of automation and support equipment [US-Canada, 2004].

A significant feature of the Italian case is that it clearly outlines how the two basic attributes of power service reliability, i.e. adequacy and security, could in some cases be somewhat contrasting. During the summer crisis of June 26, due to exceptional weather conditions, the Italian operator was unable to meet demand requirements (failure to provide an *adequate* service), while the September blackout scenario is one where the Italian system, crucially dependant from power imports, fails when this import is suddenly cut off due to a fault, thus showing a lack of overall *security*. The system operator was driven to crucially rely on imports for several reasons, among them pressure from public opinion after the summer crisis, thus operating the system closer to its capacity and security limits. Also, the deployment of the Italian crisis is largely due to premature tripping of protection relays, made to protect specific assets, like power plants, transformers, and lines: in that case, *security* in asset protection prevailed over *adequacy*, i.e. caused a total failure to meet demand.

1.1 Open questions

Market liberalisation and the creation of a single European market have changed the environment in which a secure electricity supply can be ensured. The European grid is hosting transit of commercial flows over long distances, driving system operators to become more and more inter-dependent, while at the same time substantial commercial interests have appeared and the number of market actors has significantly increased. The major political question raised by recent power outages is whether liberalisation did also trigger a process of mismanagement of the electrical infrastructure whose final outcome is an increase in the frequency and severity of power outages. As pointed out by the authoritative Eurelectric report on Power Outages in 2003 *"major power outages are viewed by consumers as a failure of the whole electricity industry, irrespective of the actual reasons and contributing factors (…) The power outage events may increase scepticism to liberalisation in citizens, and have already done so in some officials both at national and European levels"* [Eurelectric, 2004b]. In summary, there is a drive towards integration of the European electricity market, huge opportunities for advanced ICT in this domain and a need to address new vulnerability issues. The main open questions appear to be threefold:

Assessment of the socio-economic impact of blackouts[2]

We do not have adequate ways to forecast and assess the socio-economic impact of long electricity crises. Different studies, mainly based on customers' own evaluations, provide widely ranging estimates for the cost of an unsupplied kWh. Shorter outages for industrial customers are valued at highest levels (e.g. 1,000 €/kWh), while long outages (over 24 hours) are put by residential customers around 5€/kWh, and in some cases below 1€/kWh. But these estimations are to a great extent uncertain; partly due to a lack of objective approximation of actually incurred costs, and partly due to the difficulties of drawing an appropriate balance between including and excluding directly and indirectly associated damages (e.g. a longer outage of the London Underground due to safety considerations was a consequence of the otherwise short UK event) [Eurelectric, 2004b].
While the US situation had been the subject of comprehensive studies by the NERC, fully reported for instance in [US-Canada, 2004], which show that the US situation kept worsening in the last 10-15 years, data about frequency, duration and gravity of blackouts are hard to compare in Europe. The UCTE integrated data only cover the period 2000-2004, which is definitely too short to assess whether 2003 blackouts were a symptom of a pending systemic crisis, or simply exceptional events. A study would be needed to compare data over an extended period of time, encompassing liberalization, in some key European areas, e.g. United Kingdom, Scandinavia, Spain, and Italy.

Assessment of power system reliability

As extensively discussed in the previous section, many incidents arise from a pattern where the initial fault of a power system is compounded by failure of monitoring equipment and/or incorrect tripping of automatic protection devices. The general industry practice for security assessment has been to use a deterministic approach [IEEE/CIGRE, 2004]: the power system is designed and operated to withstand a set of contingencies referred to as "normal contingencies" selected on the

[2] In view of the scope of the Contract in between the JRC and the Expert, this first issue, mentioned here for sake of completeness, was not further investigated. The rest of the report deepens the other two issues.

basis that they have a significant likelihood of occurrence (. This is usually referred to as the N-1 criterion because it examines the behaviour of an N-component grid on a systematic but single contingency basis, i.e. following the loss of any one of its major components (generator, line, transformer, ect.). Load flow analysis is then applied to evaluate the resulting grid conditions and check for system limits violation. However, steady-state analysis fails to keep into account the impact of sudden disturbances and their induced transient-dynamic effect. Although innovative dynamic assessment techniques are available, these are not yet applied in the standard operators practice, as far as on-line operator support is concerned. Moreover, there is no holistic methodology for evaluating risks arising from power system failures and automation system together, so as to join physical power system risk assessment with testing/compliance control procedures for automation and protection equipment.

Review of electrical system controls

An electric system comprising interconnected power grids (regional, national and super-national) needs complex ***controls***, intended as the procedures for system management, and the related information and communication infrastructure, comprehensive of monitoring, actuation and protection devices to ensure that the delivery of electrical power anywhere in the system meets certain specified criteria. Such infrastructure has grown together with the electrical system since the ’50, and for most respects it did not go through a thorough revision after liberalisation, joint with the “pushing limits” policy induced by system limitations and constraints, so as to cope with the new security challenges. Electrical system ***controls*** appears to be no longer adequate because:

- Some alarms are not displayed on the screen of the operators that would have to manage them, due to either jurisdictional issues (e.g. along frontiers, as in the Switzerland/Italy case), or inappropriate procedures, and also because critical apparatuses are not duplicated so as to remove the effects of their malfunction (North America). In addition, there is a lack of alarm processing system that enables to identify any initial triggering event.
- In both cases the defense plan of the systems failed. Automatic protection devices were not able to avoid system collapse. Furthermore, in the Italian case, restoration was made long and cumbersome due to inadequacies of the supporting information and communication infrastructure, namely as far as emergency supply systems are concerned.

There is a growing consensus about inadequacy of the European system controls: “*The lack or inadequacy of communication, co-ordination and/or data exchange between system operators seems to have played a major role in the escalation of some of the examined events. In some cases, there was a lack of sense of urgency, so that the designed procedures were not applied. Binding rules for coordination among system operators both in normal operation and in other situations are desirable. These rules must take into account the new challenges imposed by the liberalisation and integration of the European markets (larger cross-border flows, appearance of commercial interests, etc.). Tools and means to intensify collection and availability of real-time data should be examined and established”* [Eurelectric, 2004].

TSOs in the UCTE area are still applying non-binding recommendations, which were developed before liberalisation (since 1999, a binding System Operation Agreement is in force between the NORDEL TSOs; requiring inter alia the currently valid security criteria to be observed in daily operations) [*ibidem*]. In the aftermath of the 2003 blackouts, the UCTE started an articulated revision process of its Operation Handbook [UCTE, 2004c] which is founded on the regulatory agreements among continental Europe TSOs.. The North American operational procedures alike are being revised by the NERC [2004]. Once this revision is accomplished, the Information and Communication infrastructure shall inevitably go through a redesign and reimplementation process to cope with the new regulatory agreements and the new operational procedures involved. As this infrastructure is by its nature multi-jurisdictionary, the real challenge is how to design and implement such a substantial review, which will involve all the various private and state entities that participate in the operation of the electrical system. In most of the affected countries, e.g. the US and Italy, such process is partly already in progress so as to reflect changes in the regulatory agreements between neighbouring ISOs/TSOs, which will be reasonably subsumed by the regulating authorities.

1.2 Bibliography

[AEEG, 2004] *Resoconto dell'Attività Conoscitiva in Ordine alla Interruzione del Servizio Elettrico Verificatasi il Giorno 28 Settembre 2003*, Autorità per l'energia elettrica e il gas, 9 giugno 2004 http://www.autorita.energia.it/com_stampa/index.htm

[Elkraft, 2003] *Press release: Effects of power failures must be reduced.* Elkraft, November 4, 2003, http://www.elkraft-system.dk/

[Eurelectric, 2004] *Year 2003 Power Outages: Liberalisation is not to blame, Eurelectric Report Finds*, Eurelectric Press Release, June 8, 2004, http://public.eurelectric.org/Content/Default.asp?PageID=173

[National Grid, 2003] *Investigation Report into the Loss of Supply Incident affecting parts of South London at 18:20 on Thursday, 28 August 2003, Executive Summary.* National Grid Transco. September 10, 2003. http://195.92.225.33/uk/library/documents/pdfs/London28082003.pdf

[NERC, 1997] *NERC Planning Standards*, North American Electric Reliability Council, September 1997, http://www.nerc.com/~filez/pss-psg.html.

[UCTE, 2004a] *FINAL REPORT of the Investigation Committee on the 28 September 2003 Blackout in Italy*, UCTE Ad-hoc Investigation Committee, April 27, 2004 http://www.ucte.org/pdf/News/20040427_UCTE_IC_Final_report.pdf

[UCTE, 2004b] *UCTE issues new system adequacy report 2003 with an overview of congestions on the UCTE interconnected system*, UCTE Press Release – 23 June 2004, http://www.ucte.org/pdf/News/20040623_SAR2003.pdf

[UCTE, 2004c] *UCTE Operation Handbook, Part 3, Operational Security*, UCTE, July 2004, http://www.ucte.org/ohb/e_default.asp

[US-Canada, 2004] *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, U.S.-Canada Power System Outage Task Force, April 5,

2004, http://www.nerc.com/~filez/blackout.html

2 Power System reliability and the associated methodological issues

2.1 Conceptual framework

The power system is a highly nonlinear system that operates in a constantly changing environment; loads, generator outputs and key operating parameters change continually. The system continually adjusts to small disturbances due to changing load conditions and keeps operating satisfactorily, but it must also withstand disturbances of a severe nature, like a line fault or the loss of a large generator. Large disturbances often lead to structural changes due to the isolation of the faulted elements: *"A fault on a critical element followed by its isolation by protective relays will cause variations in power flows, network bus voltages, and machine rotor speeds; the voltage variations will actuate both generator and transmission network voltage regulators; the generator speed variations will actuate prime mover governors; and the voltage and frequency variations will affect the system loads to varying degrees depending on their individual characteristics"* [IEEE/CIGRE, 2004]. For certain severe disturbances, *"interconnected systems may be intentionally split into two or more "islands" to preserve as much of the generation and load as possible. The actions of automatic controls and possibly human operators will eventually restore the system to normal state. On the other hand, if the system is unstable, it will result in a run-away or run-down situation"* and *"lead to cascading outages and a shut-down of a major portion of the power system"* [*ibidem*].

The issue of power system reliability and security, and its relationship with system stability, is debated since the 1920s, and there have been repeated attempts to establish a systematic approach to the matter by CIGRE and IEEE Task Forces, starting from the1950s until the recent deliberation issued by a joint Task Force (JTF) of the two bodies [IEEE/CIGRE, 2003, 2004]. In the fifth section of both these reports, the relationship between the concepts of power system reliability, security and stability is summarised as such:

- *"**Reliability** of a power system refers to the probability of its satisfactory operation over the long run. It denotes the ability to supply adequate electric service on a nearly continuous basis, with few interruptions over an extended time period.*
- ***Security** of a power system refers to the degree of risk in its ability to survive imminent disturbances[3] (contingencies) without interruption of customer service. It relates to robustness of the system to imminent disturbances and, hence, depends on the system operating condition as well as the contingent probability of disturbances.*
- ***Stability** of a power system refers to the continuance of intact operation following a disturbance. It depends on the operating condition and the nature of the physical disturbance."*

A summary description of how these terms have been defined and used in practice, extracted from [IEEE/CIGRE, 2003, 2004] is provided hereinafter. The reader should refer to the latter source for formal definitions of Reliability, Security and Stability.

[3] The meaning of *imminent* here is *impending* rather than *in prospect* or *overhanging*.

Stability

Both documents define Stability as *"the ability of an electric power system, for a given initial operating condition, to regain a state of operating equilibrium after being subjected to a physical disturbance, with most system variables bounded so that practically the entire system remains intact."* This definition is exhaustively motivated by the JTF: fundamental issues related to definitions of power system stability from a system-theoretic viewpoint are addressed, and a formulation of power system stability, based on general stability concepts from system theory is proposed: *"An equilibrium set of a power system is stable if, when the initial state is in the given starting set, the system motion converges to the equilibrium set, and operating constraints are satisfied for all relevant variables along the entire trajectory."* [IEEE/CIGRE, 2004]. Based on this analytical framework, the JTF report provides analytical definitions of several types of stability including Lyapunov stability, input-output stability, stability of linear systems, and partial stability. Of these various types, *"the Lyapunov stability …and asymptotic stability are the ones most applicable to power system nonlinear behaviour under large disturbances, while linear systems stability finds wide use in small signal stability analysis of power systems"*. Although power system stability is a single problem, *"the various forms of instabilities cannot be properly understood and dealt with by treating it as such. Because of high dimensionality and complexity of stability problems, it helps to make simplifying assumptions to analyze specific types of problems using an appropriate degree of detail of system representation and appropriate analytical techniques"*. This is why classification is essential for practical analysis and resolution of power system stability problems. Thus the JTF proposes the following classification, where stability disturbances are classified according to physical nature, size and originating device or process:

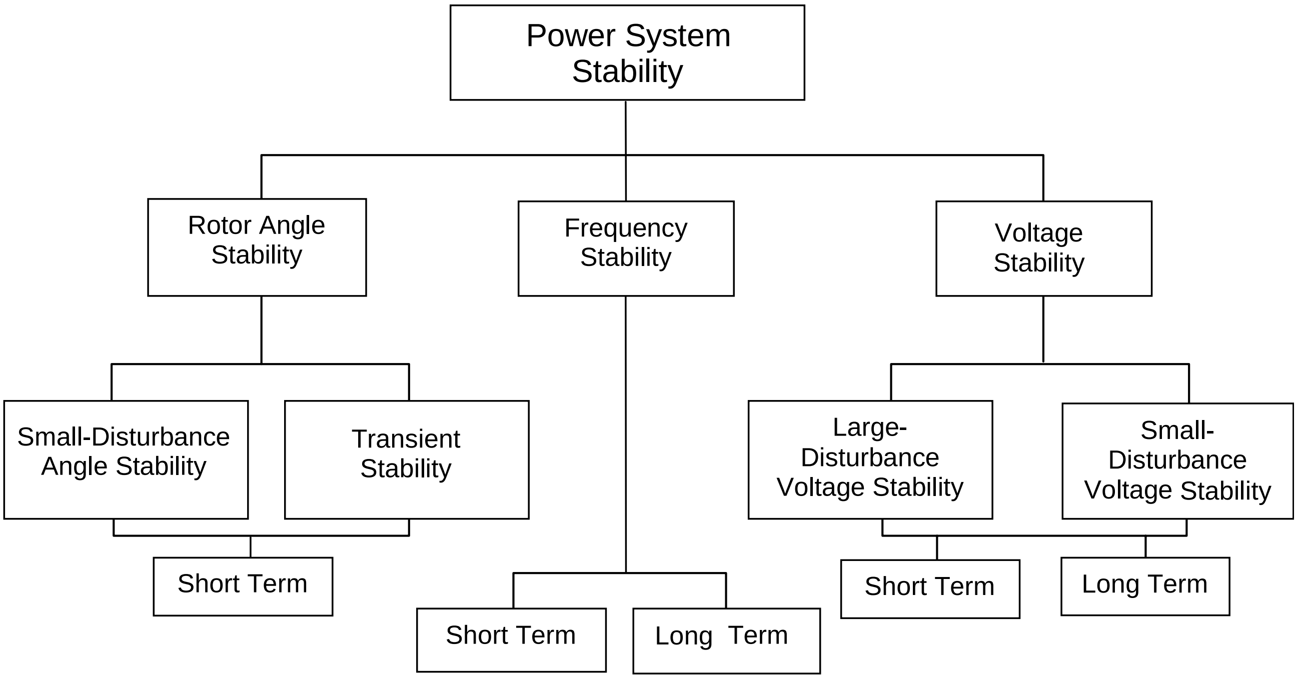


Fig. 1. *Classification of Power System Stability*

Rotor Angle Stability: these perturbations happen when some synchronous generators of an interconnected power system loose synchronism after being subjected to a disturbance. In steady-state conditions, there is equilibrium between the input mechanical torque and the output electromagnetic torque of each generator, and their speed remains constant. When this equilibrium is upset, the rotors of the machines accelerate or decelerate according to the laws of motion of a rotating body. An increasing angular shift between a faster machine and a slower one, results in the transfer of part of the load from the slow machine to the fast machine. This tends to reduce the speed difference and hence the angular separation: however, the power-angle relationship is highly nonlinear, so that, beyond a certain limit, an increase in angular shift does no longer result into an increase in power transfer, and the angular shift is further increased. Rotor angle stability events are *short term* phenomena. They are categorized as *small-disturbance rotor angle stability* phenomena when disturbances are sufficiently small that system equations can be linearised. (time frame of 10 – 20 seconds) and *large-disturbance rotor angle stability or transient stability* phenomena, due to severe disturbances, and involving large excursions of generator rotor angles (time frame of 3 - 5 seconds).

Voltage Stability: a perturbation of *voltage stability* is a progressive fall or rise of voltages of some buses of the system, and depends on the ability to maintain/restore equilibrium between load demand and load supply from the power system. A possible outcome of voltage instability is an increase of load in an area, with maximum loadability being reached, or tripping of transmission lines and other elements by their protective systems leading to cascading outages (*voltage collapse).* A major factor contributing to voltage instability is the voltage drop that occurs when active and reactive power flow through inductive reactances of the transmission network; this limits the capability of the transmission network for power transfer and voltage support. Voltage stability is classified as *small-disturbance voltage stability* (when the system is able to maintain steady voltages when subjected to small perturbations such as incremental changes in system load) and *large-disturbance* (when the system is able to restore steady voltages following large disturbances such as system faults, loss of generation, or circuit contingencies.) The time frame of interest for voltage stability problems may vary from a few seconds to tens of minutes.

Frequency Stability: a perturbation of *frequency stability* is due to active power imbalance between generators and loads irrespective of network aspects within each connected area. It can be encountered after a major disturbance has resulted in islanding. Stability in this case is a question of whether or not each island will reach an acceptable state of operating equilibrium with minimal loss of load. Instability occurs in the form of sustained frequency swings leading to tripping of generating units and/or loads. Frequency stability problems are associated with inadequacies in equipment responses, poor coordination of control and protection equipment, or insufficient generation reserve. The characteristic times of the processes range from fraction of seconds, corresponding to the response of devices such as underfrequency load shedding and generator controls and protections, to several minutes, corresponding to the response of devices such as prime mover energy supply systems and load voltage regulators.

Reliability, Adequacy and Security

According to the JTF *"Reliability is the overall objective in power system design and operation. To be reliable the power system must be secure most of the time. To be secure the system must be stable but must also be secure against other contingencies that would not be classified as stability problems, e.g., damage to equipment such as an explosive failure of a cable, fall of transmission towers due to ice loading or sabotage. Also, a system may be stable following a contingency, yet insecure due to post-fault system conditions resulting in equipment overloads or voltage violations".* NERC (North American Electric Reliability Council) [1997] defines power system reliability as *"the degree to which the performance of the elements of the system results in power being delivered to consumers within accepted standards and in the amount desired. The degree of reliability may be measured by the frequency, duration, and magnitude of adverse effects on consumer service".*

The JTF further distinguishes between two basic aspects of reliability:

- *Adequacy*: the ability to supply the aggregate electric power and energy requirements of the customer at all times, taking into account scheduled and unscheduled outages of system components.
- *Security*: the ability to withstand sudden disturbances such as electric short circuits or non-anticipated loss of system components.

As *adequacy* refers to the overall capability of the system to perform its service, it is often seen mostly as a 'static' property of the system, as opposed to *security*, which has both a 'static' and a 'dynamic' component [Bertoldi et al, 1999]. It must be noted that there is a trade-off between *adequacy* and *security*: the further the system is stretched so as to fulfill user demand, i.e. to be adequate, the closer it is pushed towards its security limits [*ibidem*]. Also according to the JTF: "*security and stability are time-varying attributes*." To assess stability, and security, one must study the performance of the power system under a particular set of conditions. *Reliability,* on the other hand, "*is a function of the time-average performance of the power system; it can only be judged by consideration of the system's behaviour over an appreciable period of time*" [IEEE/CIGRE, 2003].

A further issue is the distinction between security and stability. According to the JTF: *"system security may be further distinguished from stability in terms of the resulting consequences. For example, two systems may both be stable with equal stability margins, but one may be relatively more secure because the consequences of instability are less severe."* On this point, it is also worth noting that a more formal definition of security, based on satisfaction of a set of inequality constraints, is proposed by Dy Liacco [1968].

In summary, the relationship among the concepts pertaining power system reliability can be depicted as in Fig. 1 below:

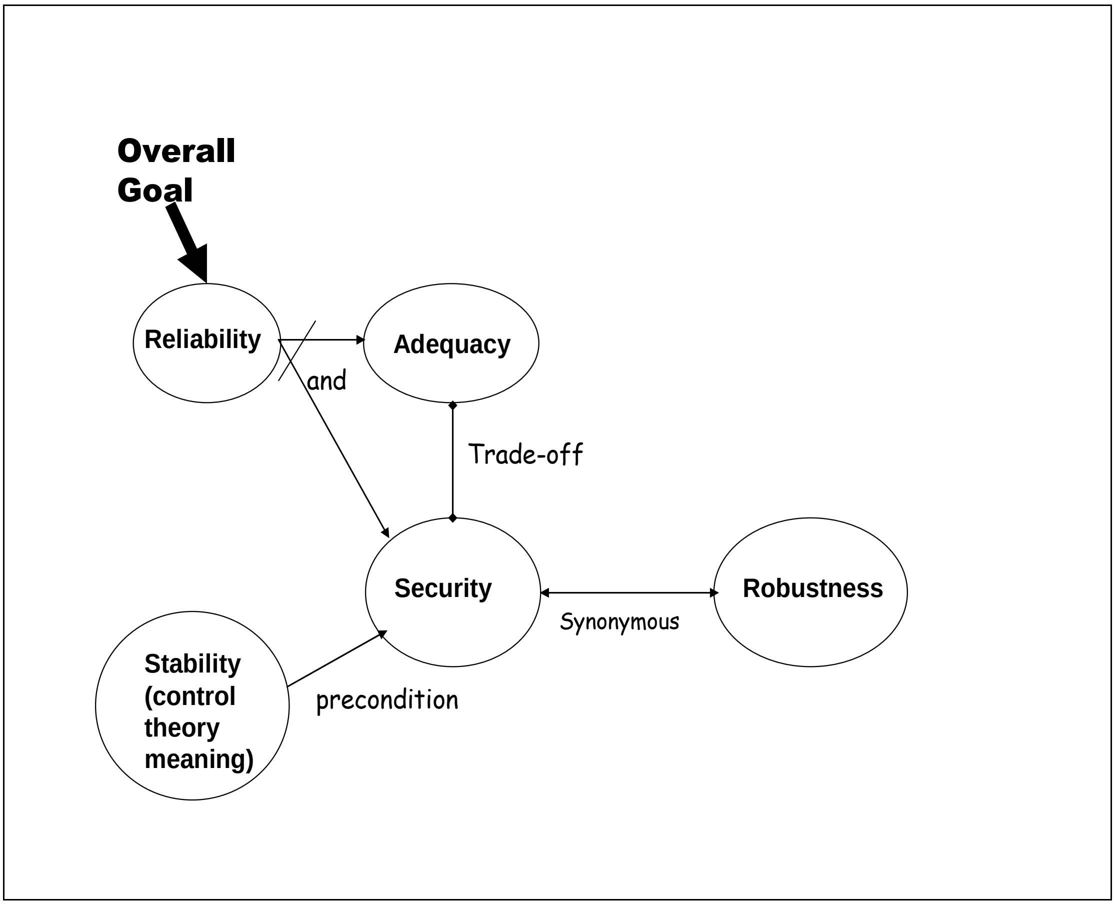


Fig. 2. *Reliability related concepts for Power Systems: Semantic Network*

It is also worth noting that, while *Reliability, Adequacy, Security* are largely used and well-defined terms in the power sector, and *Stability* is formally defined by [IEEE/CIGRE, 2004], *Robustness* is not, although it is widely used in the power sector literature more or less synonymously with Security.

2.2 Security Assessment

As implied by the conceptual framework laid down in the previous section, security assessment requires studying the behaviour of the power system under impending disturbance. There are two important components of security assessment:

- *Static security assessment:* a steady-state analysis of post-disturbance system conditions to verify that a new equilibrium point can be reached where no equipment ratings (e.g. current limits) and voltage constraints are violated.
- *Dynamic security assessment*: analysis of the different categories of system stability discussed in section 2.1, typically carried out through time domain simulations of system responses to small and/or large credible contingencies.

Hence security assessment is based on static/dynamic system simulation, with diverse models and granularity of representation.

Static Security assessment is concerned with evaluating voltage limits, thermal overloads, and generator capability limits. It usually consists in systematic verification of N-1 contingencies, and is limited to steady-state analyses. Methods and tools to assess static security, i.e. system adequacy, are since long-time in operational use, see for instance [Stott et al., 1987]. We must therefore argue that adequacy is operationally defined, in that static security of a power system can be computed through a simple, steady-state model, and rather straightforward computational techniques. However, network models and particularly which way to model external networks is still an open problem. This is a key issue in order to assess the impact of trans-national transactions on the security of a national grid.[4] In this context it is also of high relevance the problem of data sharing between TSOs, according to common simulation models and in the respect of the privacy requirements related to market liberalization.

As anticipated in the introduction, market liberalization is pushing towards an increase of exchanges, both across national borders and within each specific national market. Moreover, these exchanges become much more hectic and difficult to forecast in advance, which makes Security Assessment a key issue nowadays *[Bertoldi et al., 1999], [La Scala, 2003]*. In that respect, Dynamic Security Assessment (DSA) may become a substantial complement to static analysis, in presence of high power flows and increased risk of dynamic instabilities. However DSA crucially depends on the accuracy of the underlying model, which confirms the importance of data sharing between TSOs. DSA includes *Transient Stability Assessment* and *Dynamic Voltage Stability Assessment:* in both cases, analytic complexity (high dimensions, highly non-linear problem) may lead to combinatorial explosion (operating conditions & contingencies). As problem features typically include huge data quantity, filtering and severity ranking is performed by using qualitative and quantitative information, included operators expertise, which may involve use of Artificial Intelligence techniques [Denegri et al., 2003] [AIA, 2003]. According to Bertoldi et al., [1999], ranking criteria may be of an economic, probabilistic, and empiric nature, e.g.:

- contingency likelihood, independent from its effects;
- contingency severity, in terms of associated dynamic behaviour, topological modifications, and acceptability of the post-event operating condition;
- a combination of the above criteria, so as to rank contingencies both with respect to impending danger, and likelihood of the event.
- an overall vulnerability index, depending on (1) sensitivity to operational parameters (2) security after the first contingency until an equilibrium point is reached and (3) difficulty of the subsequent restoration process.

As earlier approaches to Dynamic Security Assessment date back to the sixties, the technology is now rather ripe for off-line operational application, while current R&D concerns integration with supervisory equipment, so as to provide on-line decision support to operators. However, the intricacies of modelling a huge non-linear system, and the complex computational procedures involved, make dynamic security assessment rather an articulate, well-approximated guess about system security, than an effective method to operationally compute dynamic security.

2.3 Power system vs. Computer Systems Dependability

Dependability of computer systems had been a concern since the foundations of this technology [Avizˇienis et al., 2001]. Computer Science views *dependability* as a global concept, encompassing such properties as:

[4] The fact that there are few attempts to cope with the problem on a continental scale is quite telling.

- *availability:* readiness for correct service
- *reliability:* continuity of correct service
- *safety:* absence of catastrophic consequences on the user(s) and the environment
- *confidentiality:* absence of unauthorized disclosure of information
- *integrity:* absence of improper system state alterations
- *maintainability:* ability to undergo repairs and modifications

Several other dependability attributes have been defined that are either combinations or specializations. For instance, security is defined as the concurrent existence of:

- *availability* for authorized users only
- *confidentiality*
- *integrity*

The widespread use of information and communication technologies made the above terminology accepted in many sectors of industry, starting from the safety critical ones: automotive, aerospace, railways, ships etc., so that it may be considered as a global concept nowadays in Control System engineering, where dependability requirements are the "*required goals of the application system in terms of the acceptable frequency and severity of the failure modes, and of the corresponding acceptable outage durations (when relevant), for a stated set of faults, in a stated environment*" [*ibidem*].

Based on this conceptual framework, several methodologies have been introduced to master the life cycle of control systems for the power system:

- quasi-formal methodologies like UML [1997-2004];
- rigorous design methodologies based on the Petri nets concept [Reisig, 1985], like Superimposed Automata, whose application was pioneered in the power sector [Ciapessoni et al., 2001];
- formal requirement specification and verification & validation methods based on logical languages [Heitmeyer and Mandrioli, 1996], like the TRIO temporal logic language experimented in the power sector by Ciapessoni et al., [1998].

Unfortunately, the conceptual framework from Computer Science was not accepted in the power sector, where a different perspective emerged long before introduction of computer systems into practical application, and was eventually established in the late nineties, as discussed in Section 2.1. This is especially confusing for control system engineers in the power sector, as they must get accustomed to switch between different terminologies, according to the specific subject and audience of their talk.

In summary, the common terms in both terminologies are:

- *Reliability:* continuity of correct service. There is no clash between the two definitions.
- *Security:* there is a substantially different, uncorrelated meaning of this term in the two disciplines. This results from the original formulation of Security in Computer Science by Laprie [1992] as *"dependability with respect to the prevention of unauthorised access and/or handling of information"*, while Power System security, as discussed, is "*the ability to withstand sudden disturbances such as electric short circuits or non-anticipated loss of system components*" [IEEE/CIGRE, 2004]. Although these definitions are deeply different, it is perhaps possible to envisage a broader definition which may encompass both concepts, see next section.

Moreover, *dependability* is a formally defined concept in Computer Science, while has no formal meaning in Power Systems Engineering, although some authors in this latter discipline take dependability as a synonymous of reliability.

The practical consequence of these different conceptions of reliability in Power Systems and Computer Science, or rather, in Control Systems engineering, is that there exist no holistic approach to risk assessment in power systems, able to evaluate the impact of control system failures aside physical components' ones. *"Devices used to protect individual equipment may respond to variations in system variables and cause tripping of the equipment, thereby weakening the system and possibly leading to system instability"*, IEEE/CIGRE, [2004] thus making automated protection equipment a key vulnerability factor in power systems. Also, as discussed in the introduction, *failure of monitoring and supervisory equipment* was a key factor, perhaps the main background cause for most recent power system outages.

2.4 Towards a holistic approach

There are recent attempts to reconcile the power system view to the global one. Holmgren et al. [2001] by the Swedish Defence Research Agency propose the following definitions:

- *Vulnerability:* the property of an infrastructure system that limits its ability to endure threats and survive accidental events that originates both within and outside the system's boundaries
- *Robustness:* a system's ability to endure threats and survive accidental events that originate both within and outside the system's boundaries, and if disturbed, return to a state where the operating characteristics correspond to the assigned function
- *Reliability:* the ability of an item to perform a required function, under given environmental and operational conditions and for a given period of time Risk: a combination of the probability/likelihood for an accident to occur and the resulting negative consequences if the accident occurs
- *Safety:* the complement of the risk concept

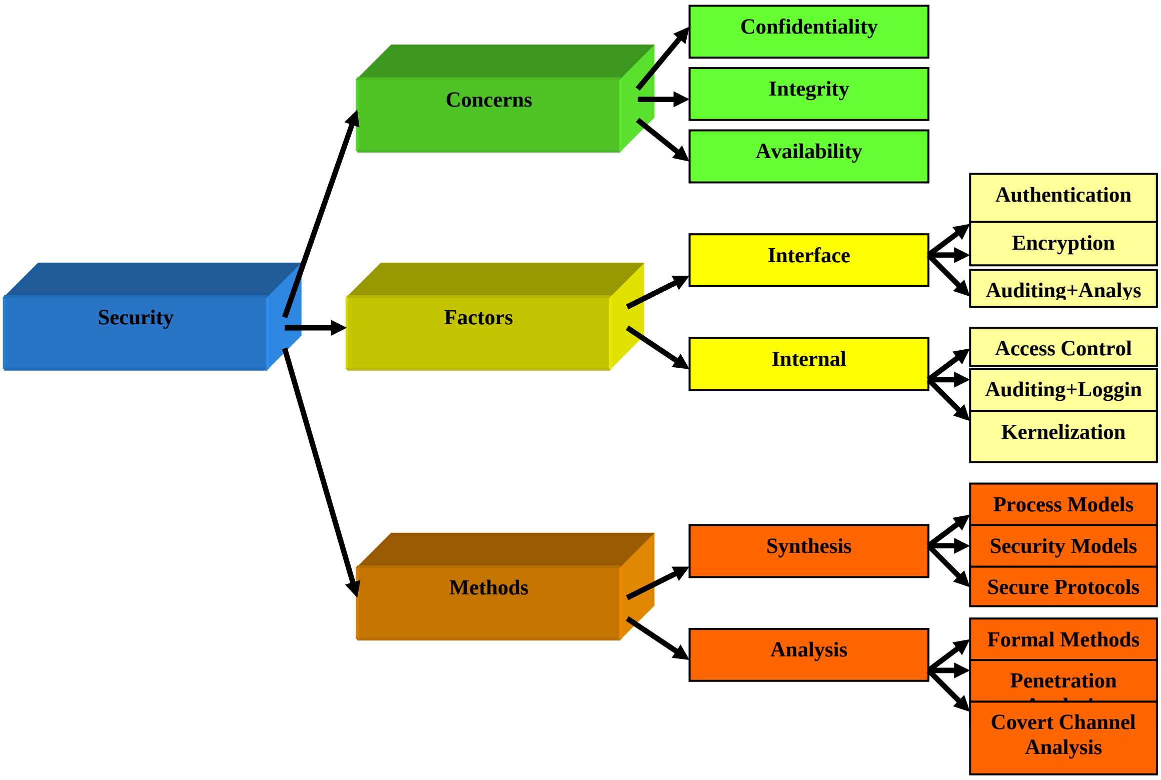
In the main, this approach is seemingly closer to the global approach to dependability, but does not really pretend to integrate the classical Power System approach. Rather, an attempt is made to establish risk analysis on a sociological base.

A unifying view might be through the recently proposed SQRA concept to define properties of a power system as a service infrastructure [Samotyi, 2003]. This approach defines:

- *Security* of power delivery and market systems as a measure of system vulnerability to natural events, human error, and intentional attack;
- *Quality* of power supplied as a measure of electric supply characteristic that can impact the performance of digital systems;
- *Reliability* of power supplied as the number of failure events and the amount of time the system is unavailable in a given year;
- *Availability* of affordable energy services as the average time per year the system is in service and is satisfactorily performing its intended function.

These definitions appear consistent with the Computer Science approach, although there is no explicit attempt to bridge the gap with the classical Power System view.

Al-Kuwaity and Kiriakopoulos [2004] provide a critical comparison of dependability related concepts in network systems and build on existing literature to provide operational definitions of five defining concepts: *Dependability, Survivability, Fault-Tolerance, Reliability,* and *Security*. Although the ample bibliography surveyed does not include references from the power sector, these definitions appear to be applicable to power systems as well. Specifically, their definition of *Security* as the *“ability to protect against undesirable events and preserve confidentiality, integrity, and availability”*, which appears broad enough to encompass Computer Science and Power System views, is taken from a paper by Barbacci et al., [2002]. What makes both works especially interesting is the taxonomy by Barbacci quoted at page 38 of the former paper:



This is especially relevant to our discussion, because it allows to position Power System synthesis and analysis methods (like Optimal Power Flow and Dynamic Security Assessment) aside to the above referred methods for Control System synthesis and analysis, like UML and Petri nets, and emerging methodologies for Information and Communication systems security assessment.

2.5 Bibliography

[AIA, 2003] *Agora, Advanced Grid Observation Reliable Algorithms,* Grupo AIA, October 2003, http://www.aia.es/internet/website_eng/Agora.html

[Al-Kuwaity and Kiriakopoulos, 2004] *Critical Analysis of Dependable, survivable, Fault-Tolerant, Reliable and Secure Network Systems,* Al-Kuwaity, M. and N. Kiriakopoulos (advising professor) Draft Dissertation Thesis, George Washington University, Dept. of Electrical and Computer Engineering, 2004.

[Avizˇienis et al., 2001] *Fundamental Concepts of Computer System Dependability,* Avizˇienis A., Laprie, J.C. and B. Randell, IARP/IEEE-RAS Workshop on Robot Dependability: Technological Challenge of Dependable Robots in Human Environments, Seoul, May 2001.

[Barbacci et al., 2002] *Distributed Real-Time Systems: Dependability, Software Reliability and Security in Critical Systems,* Andler, S.F., Lindström, B and M.R. Barbacci, University of Skövde, Distributed Real-Time Systems Course, Fall 2002.

[Bertoldi et al., 19xx] *Affidabilità e sicurezza del sistema elettrico in regime di mercato elettrico competitivo*. Bertoldi O., Invernizzi A., Rivoiro A. and P. Scarpellini, AEI workshop on " Techno-Economic Optimisation of Power Generation and Transmission Systems in the frame of a Liberalised Market", Rome, Sept. 29, 1999.

[Ciapessoni et al., 2001] *Partitioning of Hierarchical Automation Systems,* Ciapessoni, E., Crespi-Reghizzi, S., Maestri, F., Ornstein, A., Psaila, G., and J. Szanto, 13th Euromicro Conference on Real-Time Systems, Delft, The Netherlands. June 2001.

[Ciapessoni et al., 1999] *From formal models to formally based methods,: an industrial experience,* Ciapessoni, E., Coen-Porisini, A., Mandrioli, D., Morzenti, A., and P. Mirandola, ACM Transactions on Software Engineering and Methodology Vol. 8 , Issue 1, Jan. 1999) pp: 79 – 113.

[CIGRE, 1997] *Power System Security Assessment: A Position Paper,* CIGRE TF 38.03.12 Report Electra, No. 175, December 1997.

[Denegri et al., 2003] La sicurezza dei sistemi elettrici per l'energia. Aspetti metodologici e tecnologici sviluppati in due progetti europei: OMASES ed EXAMINE, Denegri, G.B., Invernizzi, M., Lucarella, D., Massucco, S. e A. Morini, Convegno Scientifico Nazionale "Sicurezza nei sistemi complessi", Bari, October 2003.

[Dy Liacco, 1968} Control of Power Systems via the Multi-Level Concept, Dy Liacco T.E., Case Western Reserve University, Systems Research Center, Report SRC-68-19, June 1968.

[Elkraft, 2003] *Press release: Effects of power failures must be reduced.* Elkraft, November 4, 2003, http://www.elkraft-system.dk/

[Heitmeyer and Mandrioli, 1996] *Formal Methods for Real-Time Computing,* Heitmeyer, C.and D.

Mandrioli, editors, Vol. 5 of Trends in Software. Wiley, 1996.

[Holmgren et al., 2001] *Vulnerability of Complex Infrastructures - Power Systems & Supporting Digital Communication Systems,* Holmgren, Molin & Thedéen joint with the Centre for Safety Research, Stockholm, 5th International Conference on Technology, Policy & Innovation, Delft, NL, June 2001.

[IEEE 1978] *Reliability Indices for Use in Bulk Power System Supply Adequacy Evaluation,* IEEE Working Group Report, IEEE Trans. on Power Apparatus and Systems, Vol. 97, No. 4, pp. 1097-1103, July-August 1978.

[IEEE/CIGRE, 2003] *Overview on Definition and Classification of Power System Stability*, IEEE/CIGRE Joint Task Force on Stability Terms and Definitions, CIGRE/IEEE-PES International Symposium on Quality and Security of Electric Power Delivery Systems, Montréal, Canada, October 7-10, 2003.

[IEEE/CIGRE, 2004] *Definition and Classification of Power System Stability*, IEEE/CIGRE Joint Task Force on Stability Terms and Definitions, IEEE Transactions on Power Systems, 1387- 1401, Vol. 19, Issue 3, Aug. 2004, ISSN: 0885-8950.

[La Scala, 2003] *Sicurezza delle infrastrutture elettriche: prospettive di ricerca,* M. La Scala, Convegno Scientifico Nazionale "Sicurezza nei sistemi complessi", Bari, October 2003.

[Laprie, 1992] *Dependability: Basic Concepts and Terminology***,** J. Laprie (ed), Springer-Verlag, New York, 1992.

[Reisig, 1985] *Petri Nets : an Introduction*, W. Reisig, Springer-Verlag, EATCS, 1985.

[Samotyi, 2003] *Power System Infrastructure for a Digital Society: Creating the New Frontier,* M. Samotyi, CIGRE Symposium on Quality and Security of Power Delivery Montreal, 2003.

[Stott et al., 1987] *Security Analysis and Optimisation,* Stott, B., Alsac O., and A.J.Monticelli Proceedings IEEE, vol. 75, n. 12, December 1987.

[UML, 1997-2004] *UML™ Resource Page,* Object Management Group, Inc , 1997-2004, [http://www.uml.org/]

3 Review of power system controls

3.1 Introduction

As discussed in the Introduction to this report, the blackout events of Summer 2003 have pointed out the inadequacy of power system controls (intended in the threefold meaning of operating procedures for interaction among stakeholders, manual control and automatic control). As this inadequacy is quite patent to operators, the blackouts have triggered a hastened review of the whole control system, which may in turn bring about new vulnerabilities.

To analyse this process in detail, we need first to overview briefly the current state of power system controls, so as to point out specific inadequacies highlighted by the blackout events. To do so, we will focus first on a basic principle of power system control, primary and backup relying, and provide later an introduction to power system defense plans, taking the Italian situation as a paradigm. This overview does neither pretend to be comprehensive nor detailed (a comprehensive, detailed analysis of the current state of the art of power system controls would probably require several books). The key to this overview is rather to provide the minimum background information needed to understand the reasons for the two major blackouts of 2003, the American North East and the Italian one. The central section of this part of the report provides an analysis of these two blackout events.

Then we introduce the emerging technologies in the power system control sector, Special Protection Systems, Wide Area Measurement, and Adaptive Protection. Although these technologies started to be introduced in the mid eighties, they are not yet fully mature. Moreover, their integration within the existing legacy control system is on the frontier of current research in the sector. We will show how this integration is very demanding, to the point of leaving a number of basic issues unsolved:

1) To which extent future control systems can be automated? Although most control decision need to be automated, due to the strict real time requirement, yet the system must retain enough flexibility, which requires keeping humans in the loop.
2) Which way will the operator of the control room of the future supervise the power system? As current technologies permit to integrate more functions (operational supervision, administrative and business functions etc.), which way will we manage this integration, and which way will the system be operated?
3) The complexity of the new technologies, which are highly ICT intensive, may bring about new vulnerabilities. Which way to master this complexity?

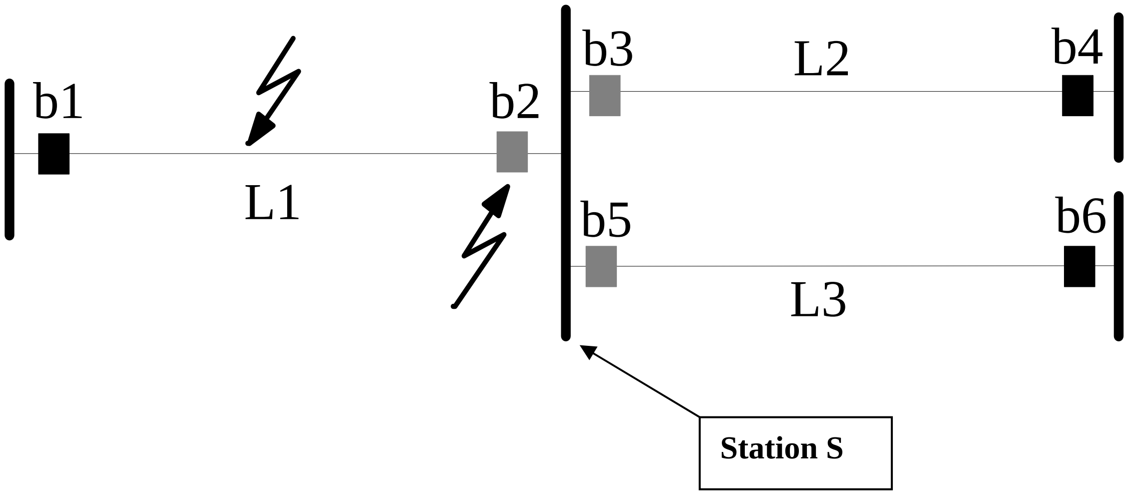
3.2 Background on power systems controls

Primary and backup relaying

Protection against short circuits is achieved by two groups of relaying equipment: primary relaying and back-up relaying. Primary relaying is the first line of defense, whereas back-up relaying works only when primary relaying fails. Back-up relaying is employed only for protection against short circuits. These are the preponderant type of power failure, hence short primary relaying is more likely to fail than other protections, due to several reasons (current or voltage supply to the relays, protective relays, tripping circuit or breaker mechanism, etc.).The main design principles for primary and backup relaying in protection systems are the following [Russell Mason]:

1. Circuit breakers are located in such a way as to disconnect only one faulty element.
2. A separate zone of protection is established around each system element. Any failure occurring within a given zone will cause the tripping of all and only the circuit breakers within that zone.
3. For failures within the region where two adjacent protective zones overlap, more breakers will be tripped than the minimum necessary. In fact, if there were no overlap, a failure in a region between zones would not lie in either zone, and therefore no breakers would be tripped.

'*Back-up relaying is located so that anything that might cause primary relaying to fail will not cause failure of back-up relaying as well, i.e. so as not to employ or control anything in common with the primary relays that are to be backed up. So far as possible, the practice is to locate the back-up relays at a different station. Consider, for example, the back-up relaying for breaker b2 on the transmission line L1 of Fig. 2. Its back-up relays are normally arranged to trip breakers b4 and b6. Should breaker b2 fail to trip for a fault on the line L1, breakers b4 and b6 are tripped; breakers b4 and b6 and their associated back-up equipment, being physically apart from the equipment that has failed, are not likely to be simultaneously affected as might be the case if breakers b3 and b5 were chosen instead'*



The back-up relays at locations b1, b4, and b6 provide back-up protection if bus faults occur at station S. Also, the back-up relays at b1 and b4 provide back-up protection for faults in the line L3. In other words, the zone of protection of back-up relaying extends in one direction from the location of any back-up relay and at least overlaps each adjacent system element.
When back-up relaying functions, a larger part of the system is disconnected than when primary relaying operates correctly. This is inevitable if back-up relaying is to be made independent of those factors that might cause primary relaying to fail. Moreover, back-up relying must operate with sufficient time delay so that primary relaying will be given enough time to function. In other words, when a short circuit occurs, both primary relaying and back-up relaying will normally start to operate, but primary relaying is expected to trip the necessary breakers to remove the short-circuited element from the system, and back-up relaying will then reset without having had time to complete its function. When a given set of relays provides back-up protection for several adjacent system elements, the slowest primary relaying of any of those adjacent elements will determine the necessary time delay of the given back-up relays'. [*ibidem*].

Distance relays are adjusted on the basis of the impedance between the relay location and the fault location. The first, high-speed, zone of distance relays is adjusted in such a way as to *reach* to 80% to 90% of the length of a two-ended line. The overall *fault clearing* time of a distance protection depends on:

1. the time required to measure the impedance;
2. the time needed to issue the command to the breaker;
3. the opening time of the breaker;
4. the residual arcing time,

and amounts to 40-50 msec. in state-of-the-art equipment.
The purpose of the second-zone unit of a distance relay is to provide protection for the rest of the line beyond the reach of the first-zone unit. It is adjusted to operate even for arcing faults at the end of the line. To do this, the unit must reach beyond the end of the line. It to try to have the second-zone unit reach is customary to reach at least 20% of an adjoining line section.. *This second-zone time is normally about 0.2 second to 0.5 second.*

The third-zone unit provides back-up protection for faults in adjoining line sections. So far as possible, *its reach should extend beyond the end of the longest adjoining line section* under the conditions that cause the maximum amount of underreach. *The third zone time delay is usually about 0.4 second to 1.0 second.* [5]

[5] Most distance protections are equipped with power swing blocking relays. These disable protection trip for stable oscillatory overloads while enable it when the area is getting out of step with respect to neighbouring areas (this latter function is activated for distance protection over lines connecting different areas).

As noted in chapter 2.1, there is a trade-off between adequacy and security of a power system. This conflicting set of objectives also applies to protection systems, where [Sidhu and Rosas, 2003]:

- *adequacy*[6] is a measure of the protection system to perform properly in removing system faults;
- *security* is a measure of the protection tendency in not initiating an incorrect trip action.

Security may be enhanced, for instance, by utilising redundant relays, and issuing the trip command when any of the relays detects a fault. This trade-off has an economic facet as well: to ensure the *security* of asset protection systems – either for transmission lines or power generators – means to adjust relays for ensuring their operation when the security of the asset is menaced by an over-current or by a low rotating speed, respectively. This objective may conflict with ensuring an *adequate* power service. An over-cautious protection setting may cause, for instance, distance protections to trip in the third zone when the current, although high, does not correspond to short circuit in neighbouring lines yet. This is what happened in most blackouts, and namely in the American Northeast - August 2003, and the Italian one in September, as discussed in the next chapter 3.3.

Defense Plans

All control actions (both manual and automated) to prevent a power system to pass from a normal condition to an emergency condition, or to restore it into a normal condition from an emergency condition, are usually defined as Defense Plans. Manual control actions in response to a complex event, which usually generates a large number of alarms, require at least 10' to be operated. When response times need to be shorter, automated control devices are required. These may be either local, like most protection systems, or involve a more complex logic.

To provide a brief overview of current defense plans, from now on we will focus on the ones in use on the Italian system [GRTN, 2000]. In view to provide insights about their vulnerabilities, this is a reasonable choice to fix ideas, as the Italian system is one of the most stressed, due to its overall imbalance, caused by its high dependency on power imports from neighbouring regions and its antenna-like structure.

Critical Section Control

A critical section is defined as a set of 380 kV lines whose loss would result into separation of a portion of the grid. Critical section control is meant to avoid separation by detaching some load after a number of lines have been eventually opened by the relevant line protection. The load detached by critical section control is the minimum required to avoid separation of a portion of the grid and the subsequent triggering of the Automated Load Shedding Plan described in the following section.

Critical section control is operated by the EDA automated detachment system. The input signals to this system are:

[6] The authors actually use the term *dependability* instead of *adequacy* which further testifies the terminology maze in the sector.

- the breaker state on each line (this signals whether the line is operational),
- whether active power through that line did trespass a lower threshold,
- whether active power did trespass a higher threshold on that same line,
- whether the line protection did operate.

The triggering conditions for the main control logic of the EDA are:

- two lines of the critical section are out of service and the higher threshold was trespassed on a single line currently operational,
- three lines are out of service and the lower threshold was trespassed on a single line in operation.

One second after one of these conditions becomes true, the EDA sends a remote control signal to the emergency load detachment banks.

Although this logic is very simple, the thresholds were set after studying the grid behaviour both in static and dynamic conditions under several different grid set ups and several different power import conditions. Basically, critical section control has to ensure that:

- Line overload shall not go beyond 140% the security limit for any 220 and 380 kV.
- Voltage on any line shall not go below prefixed limits, and the grid shall not be affected by an unstable behaviour.
- Any line protection shall not be triggered due to the dynamic behaviour of the grid after EDAs’intervention.

The currently operational EDA systems regard:

- Control of the critical section on the critical section embracing all Italian northern borders Control of France-Italy connections
- Control of the critical section between Northern Italy and Central Italy
- Control of the critical section between continental Italy and Sicily

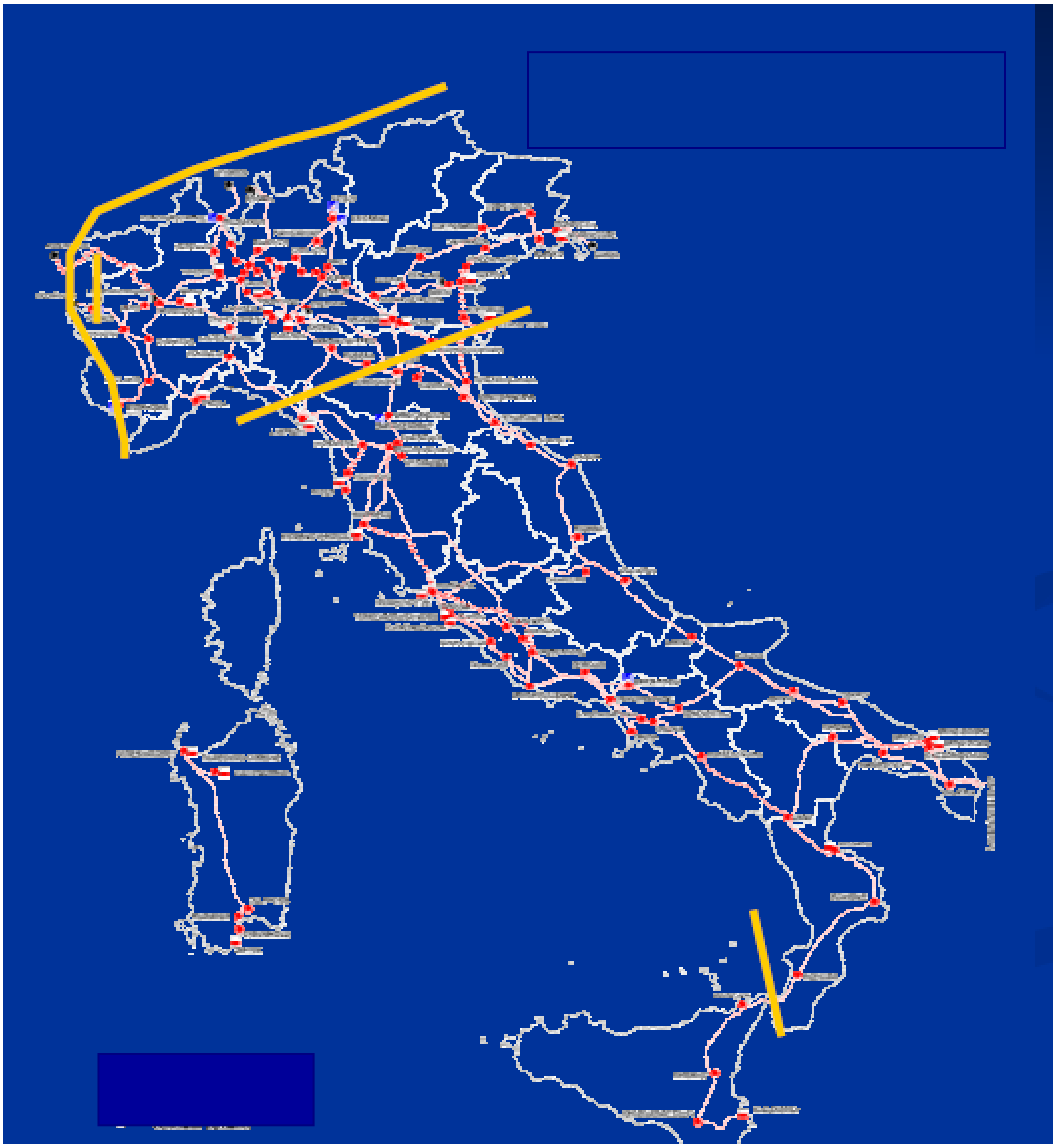


Fig 3 – Italian grid's critical sections.

Load Shedding

When two areas of the grid get separated, the area importing energy has not enough generating capability so that its frequency slows down, and the area quickly collapses. The Load Shedding plan is to avoid that frequency gets below a value which is considered to endanger power generating plants. In the Italian system this value is specifically set to 47.5 Hz, according to UCTE provisions [UCTE, 2003]. When frequency remains below 47.5 Hz for 4", thermal power production plants are allowed to separate from the grid ('Load rejection').

The load shedding plan results into detachment of a load amount depending on frequency value and its derivative. For ordinary loads, frequency thresholds are set between 49.6 e 49.0 Hz, and frequency derivative thresholds are set between 0.2 e 0.5 Hz/sec. For pumps frequency thresholds are set between 49,1 e 47,7 Hz, and frequency derivative thresholds between 0,05 and 0,50 Hz/sec. An appropriate combination of these thresholds results into shedding of 3-5% of the total load amount for each shedding step. The overall amount of load to be shed is 70% of the total. Load shedding relays have frequency activation threshold at 49.1 Hz. Load shedding is operated on the MV distribution grid but: this allows selecting loads to be detached, while this would be impossible on the transmission grid. The system goal is to shed 60% of the total load, a further 10% is added up to take into account unavailability and malfunctions of the load shedding relays and the breakers operated by the system.

As discussed, when frequency goes below 47.5 Hz, all thermal power plants would automatically reject load, and the whole system would collapse. To avoid a generalized blackout, a few small power generating station close to broad cities get separated from the grid together with the neighbouring grid serving that city.

In some grid areas, the collapse of a single line may result into power generation capacity exceeding demand. In case the power plant is not equipped with an automatic regulatory control system, the power generating group must be remotely controlled so as to reduce load. To avoid economic losses in large power stations, a few generating groups are equipped with event based load rejection systems. These are activated in case one or more lines are lost. This strategy can be implemented either by remote activation, or by appropriate manual set-up of the automated plant control systems.

Manual Defense Plans

When the power system is affected by slow dynamic phenomena (see Section 2.1), mostly related to voltage degradation, power system operators may manually operate the system by blocking transformers tap changing towards power distribution and by selectively detaching loads via the Emergency Operating Console (this latest manoeuvre is operated when all other corrective actions at a local and national level could not withstand the voltage collapse trend).

Automatic tap changing in 380/150-132 kV and 220/150-132 kV autotransformers and AT/MT transformers allows continuous regulation of secondary voltage levels. This is usually operated through an automatic control, but may be also manually operated by the plant operator. This is done either in accordance to a daily plan agreed between the ISO/TSO and the plant operator or under direct command by the ISO/TSO. When there is slow voltage degradation, the system operator may impose total or partial blocking of transformer tap changing, in order to avoid that automatic regulatory control results in further voltage degradation in the 380/220 kV transmission grid.

The ISO/TSO operating control centres are equipped with Emergency Operating Consoles that are to manually operate load detachment by selectively graduating its amount and location. These Consoles are load detachment matrices composed by 30 push-buttons (6 groups of 5 push-buttons) plus 5 overall area push-buttons operating 5 individual push-buttons. While the individual push-buttons are to detach load on a rather small district, area push-buttons operate load detachment on a large region.

In exceptional cases, a large portion of the electric grid may be affected by a long term generation inadequacy. In those cases the ISO/TSO resorts to a plan to cyclically partition load detachment

(PESSE, Italian acronym for Electric System Emergency Security Plan).
To this aim the HV power grid is provided with ad-hoc equipment to partly automate these load detachment manoeuvres.
The Plan is executed by distribution companies in accordance with ISO/TSO instructions. Distribution companies are to define the Plan as far as their customers are involved, and must establish the ways, the amount and the localization of load detachment, the relevant timetable and all manoeuvres in order to operate load detachment and return to normal operating conditions. When power generation inadequacy may be forecast a few hours in advance, the Plan involves execution of a selective programme to dilute load detachment on a large number of end-users, so as to by-pass automatic response of the equipment. When the emergency condition cannot be forecast, this Plan may be operated soon after equipment automatic response, so as to dilute the impact on a wider number of end-users. Households are mostly involved during daylight, while impact on large power consumers, like process industry and manufacturing is delayed until 16 to 20-22 in the evening.

3.3 Focus on the blackouts

This section provides a comparative analysis of two major recent blackouts, The American North East blackout (August 14, 2003), and the Italian blackout (September 27-28, 2004). These events were by far the largest in the current century, had profound and lasting impact on the public, and are one main motivation for this study. A comprehensive and authoritative overview of most recent blackouts is provided by the Eurelectric Task Force on Power Outages [Eurelectric, 2004]. The reader may also refer to a previous JRC report [Stefanini, 2005] to find more details on these events as well as on other recent blackouts in Europe.

The American North East blackout

The Eastern part of the US grids supplies about 2/3 of US consumers. The market is open to retail competition. The grid is inadequate to the competition regimen, because it was designed long time ago – no hint of a competitive market. In the area where the NE blackout started, basically the US portion of the Great Lakes basin, there are several transmission system operators, 3 of them in the Ohio state only. 50 Million people were affected. Blackout lasted 1 day in New York and 2 in Detroit. Hence the situation basically matches the Italian one in terms of figures, although restoration was quicker in Italy.
The final report of the joint *ad-hoc* US-Canada investigation committee on the blackout [US-Canada 2004] evidenced the following groups of causes for the event:

> The Ohio phase of the August 14, 2003, blackout was caused by deficiencies in specific practices, equipment, and human decisions by various organizations that affected conditions and outcomes that afternoon—for example, insufficient reactive power was an issue in the blackout, but it was not a cause in itself. Rather, deficiencies in corporate policies, lack of adherence to industry policies, and inadequate management of reactive power and voltage caused the blackout, rather than the lack of reactive power. There are four groups of causes for the blackout:
> Group 1: *FirstEnergy and ECAR failed to assess and understand the inadequacies of FE's system,*

particularly with respect to voltage instability and the vulnerability of the Cleveland-Akron area, and FE did not operate its system with appropriate voltage criteria. (Note: This cause was not identified in the Task Force's Interim Report. It is based on analysis completed by the investigative team after the publication of the Interim Report.)

A) FE failed to conduct rigorous long-term planning studies of its system, and neglected to conduct appropriate multiple contingency or extreme condition assessments.

B) FE did not conduct sufficient voltage analyses for its Ohio control area and used operational voltage criteria that did not reflect actual voltage stability conditions and needs.

C) ECAR (FE's reliability council) did not conduct an independent review or analysis of FE's voltage criteria and operating needs, thereby allowing FE to use inadequate practices without correction.

D)Some of NERC's planning and operational requirements and standards were sufficiently ambiguous that FE could interpret them to include practices that were inadequate for reliable system operation.

Group 2: *Inadequate situational awareness at FirstEnergy. FE did not recognize or understand the deteriorating condition of its system*.

A) FE failed to ensure the security of its transmission system after significant unforeseen contingencies because it did not use an effective contingency analysis capability on a routine basis.

B) FE lacked procedures to ensure that its operators were continually aware of the functional state of their critical monitoring tools.

C) FE control center computer support staff and operations staff did not have effective internal communications procedures.

D) FE lacked procedures to test effectively the functional state of its monitoring tools after repairs were made.

E) FE did not have additional or back-up monitoring tools to understand or visualize the status of their transmission system to facilitate its operators' understanding of transmission system conditions after the failure of their primary monitoring/alarming systems.

Group 3: *FE failed to manage adequately tree growth in its transmission rights-of-way.*

This failure was the common cause of the outage of three FE 345-kV transmission lines and one 138-kV line.

Group 4: *Failure of the interconnected grid's reliability organizations to provide effective real-time diagnostic support*.

A) MISO did not have real-time data from Dayton Power and Light's Stuart-Atlanta 345-kV line incorporated into its state estimator (a system monitoring tool). This precluded MISO from becoming aware of FE's system problems earlier and providing diagnostic assistance or direction to FE.

B) MISO's reliability coordinators were using non-real-time data to support real-time "flowgate" monitoring. This prevented MISO from detecting an N-1 security violation in FE's system and from assisting FE in necessaryì relief actions.

C) MISO lacked an effective way to identify the location and significance of transmission line breaker operations reported by their Energy Management System (EMS). Such information would have enabled MISO operators to become aware earlier of important line outages.

D) PJM and MISO lacked joint procedures or guidelines on when and how to coordinate a security limit violation observed by one of them in the other's area due to a contingency near their common boundary.

Source: US-Canada [2004]

The US situation was an N-2, perhaps an N-3 one, i.e. three major failures had to happen prior to system collapse. When the first line, Stuart-Atlanta, tripped at 14:02, the other surrounding ones had to bear the additional load. The second failure (Chamberlin-Harding) happened one hour after the first; the third (Hanna-Juniper) after another half an hour. Hence there was plenty of time to counteract the contingencies. Then the collapse was rather sudden. Blackout actually started at 16:06, about half an hour after the third event. By 16:10 the whole lake region was affected. New York was hit at 16:13.

When the cascade of events was started, a number of concurrent issues have to be pointed out:

- protections systems proved to be inadequate: about 70% did not work properly;
- inadequate or faulty SCADA and EMS: First Energy lost its alarm processing system until a few minutes before the first event. Awhile the other neighbouring operator, MISO had an independent software problem;
- there was insufficient reactive power support and operators were unable to counteract;
- system operators (PJM, MISO, etc.) need to coordinate their defense plans;
- planning studies are insufficient;

In summary, the numerous causes and contributing factors can be grouped into four categories:

1. inadequate management of tree growth in transmission rights-of-way
2. inadequate situational awareness
3. inadequate diagnostic support
4. inadequate system understanding

Apart from the triggering event, due to 1, the whole deployment of the crisis is almost entirely due to concurrent unreported failures both of FE's supervisory system and of the diagnostic equipment (the state estimator) available at MISO, the regional TSO. In turn, this was the main cause for the inadequate situational awareness at First Energy and MISO. Failure to provide backup to this equipment can hardly be understood in the context of such a complex and hazardous supervisory task – when compared with security standards applied in the energy sector in Europe and to other safety critical processes almost everywhere.

The Italian blackout

Starting at 3:01 on the night of September 28, an event originated in Switzerland resulted into a blackout which affected the whole of Italy except Sardinia. Italy was importing about a quarter of the domestic consumption (including big pumped storage plants) through fifteen transmission lines from France, Switzerland, Slovenia and Austria, when a main line in Switzerland through the Lukmanier pass, tripped due to a tree flashover. *After re-connection failed,* failing to recognise the overloading of the remaining lines, *the Swiss grid operator called the Italian operator for a 300 MW decrease in import..* In twenty four minutes, a second Swiss line through the S.Bernardino pass tripped, initiating a cascade tripping of all transmission lines along the Italian border. In two and a half minutes, Italy went into a total blackout.

The event took place on Saturday night, when nearly all productive activities were at rest, thus resulting into limited impact on the population and the economy. Nevertheless energy restoration required from 3 to 19 hours, 3-4 hours for the northern of Italy up to 19 hours for Sicily. However, as the blackout took place on a Saturday night, in addition to limiting direct damage, also made event management simpler by guaranteeing high mobility of event management and rescue teams. On both respects, a blackout during a working day might result into a completely different scenario. Nevertheless, it was the largest blackout in Europe since ever, at least in peace times, comparable in size with the American North East event (about 170,000 versus 350,000 MWh estimated energy not supplied; 50 million people involved).

Immediately after the blackout, transmission system operators' executives of the five involved countries decided to set up an independent UCTE Investigation Committee that was given the mission to bring a transparent and complete explanation of the blackout to the national and European Authorities and to the general community. The Committee conclusions are summarised below:

The Committee identified four main reasons for the fact that things did not go as foreseen:
1. Unsuccessful re-closing of a first line in Switzerland (Lukmanier) because of a too high phase angle difference
Due to the high loads on the remaining lines, an automatic device, aiming at protecting the equipment, blocked according to its design settings the possibility of restoring the line back into service.
2. Lacking a sense of urgency regarding the overload of a second line connecting the Swiss system to Italy (San Bernardino) and call for inadequate countermeasures in Italy
The operators were unaware of the fact that the overload was only allowable for about 15 minutes. A single phone call by ETRANS took place 10 minutes after the trip of the first line. ETRANS asked for the imports to be decreased by 300 MW. This measure was completed by GRTN within 10 more minutes. Even together with the Swiss internal countermeasures, it was insufficient to relieve the overloads.
3. Angle instability and voltage collapse in Italy
This was the reason why the Italian system collapsed after its separation from the UCTE system. It was not the cause of the origin of the event.
4. Right-of-way maintenance practice
Tree cutting, to maintain safe distances regarding flashover, is subject to national regulation" *(NdA: this is to remark that responsibility over the primary cause of the event is stipulated by national regulations which look to be inadequate and/or not properly enforced,).*
Source: UCTE [2004a]

A separate issue from investigation on the reasons why the triggering event chain of the blackout was inadequately dealt with, is why the Italian system collapsed, once isolated from the UCTE grid, and why restoration was so cumbersome. In its final report on the event [AEEG, 2004], the Italian authority for Electricity and Gas performs an analysis for what regards the reasons for the Italian system collapse and its long restoration:

E4. Missing adoption of the foreseen (i.e., UCTE) countermeasures has resulted in the inefficiency of the control logic of the critical sections to defend the integrity of the net in front of cross-border interconnections (…) on September 28, 2003, missing adoption of the foreseen countermeasures has determined a chain of events which made ineffective the automatic control of the critical section Rondissone-Albertville and of the foreign critical section.
E5. The separation of the national electrical system from the UCTE grid has been characterised by phenomena of transient instability of the Italian electrical system with respect to the UCTE grid.
E6. As a result of the separation of the national electrical system from the UCTE grid, the spread of service interruptions in the national territory has been caused from a series of concurrent events: primarily, the anticipated separation of power generation units with respect to the prescribed terms and, second, an ineffective reaction of the load separation system
E7. During the service interruption spread phase the behaviour of 21 power generating groups was

patently different from what established in the technical Rules of connection to the national transmission grid.
E8. The whole automatic load shedding action did not comply with the levels established by the technical connection Rules. Moreover, several distributors connected with the national transmission grid were not equipped with automatic load shedding devices.
E9. The rate of failure of the load rejection actions by power generating groups was very high . This seriously compromised service restoration.
E10. In most cases the independent start of the first blackstart units did not take place. The GRTN managed the service restoration only through the lines connecting the North to the rest of Italy. This caused the remarkable delay of service restoration in the Center and South regions
E11. During the service restoration phases, the telecommunication systems for remote control of manoeuvre of components of the national transmission elements grid endured phenomena of instability and saturation. Moreover, the emergency supply system of the above telecommunication systems resulted inadequate.(…) From hours 08:00 to hours 14:40, it was impossible to use the foretold automatic control system because of lack of supply, due to inadequacy of the emergency supply systems of the relevant telecommunication systems. This required the use of a backup satellite telecommunication system and to manually operate the restoration, thus compromising ready restoration of service.
English translation from AEEG [2004]

The degradation of the Italian system and the causes of its long restoration are mostly due to either inadequate or inappropriate behaviour of protection equipment. All three categories of protection systems:

1. critical section control
2. load relief equipment
3. load rejection equipment

failed for different reasons. It is also remarkable that 21 out of 52 power plants failed to compensate the lack of imported power, because most of them rejected load well above the stated threshold of 47.5 hertz. This highlights an important issue: the need to enforce the general rules that determine the security of the electric power infrastructure.
In conclusion, a key concept in power systems defense is the one of **critical sections**. In Italy, 13 critical sections were identified by Enel in the 80’s. In case of topological weakness, the criticality condition is activated for that section; if, in such condition, another line belonging to that section trips, automatic load shedding is activated; this is triggered by opening of the breakers of the interconnection lines on the Italian side only. This is why it did not work in the last blackout.
In practice, each critical system control activates its own load shedding plan. The main drawback of such a choice in a highly interconnected grid is that load shedding in one regional area may result into unbalancing other areas. For this reason, set up of load shedding thresholds is based on sensitivity analysis. After liberalization, this resulted into a considerable drawback, because load shedding systems operate on MV distributions, hence they are under jurisdiction of several power distribution utilities. Hence the load shedding control scheme was not updated according to up to date sensitivity analysis, resulting into system inadequacy.
According to the Italian grid code, generators have to keep connected for f ≥ 47.5: 21 generators (16% of the total generation power) tripped in advance,. Moreover, 8/140 generators only succeeded in the load rejection procedure.
Restoration was made long and cumbersome due to failure of telecommunication equipment, which

put most remote control systems out of operation. In turn, this was due to inadequate dimensioning of the backup supply of telecom equipment, which granted continuity of operation for 1-2 hours.

Comparison between the US and the Italian blackout

In conclusion, the two major blackouts overviewed show a similar basic pattern:

1. Multiple interacting contingencies – no single cause;
2. A low probability event sequence, very difficult to predict;
3. In both cases, the triggering event was compounded by failures of the monitoring, control and protection equipment failed, so that, once the entire cascade of events unfolded, operators could not counteract - time was too short.

However, two important differences are to be remarked as well:

1. The Italian blackout had a cross border cause in Switzerland. While Italian operators were unaware of the mechanics of the event due to the inadequacy of the current UCTE procedure for dealing with cross border events, the US case deployment was mostly due to failure of the monitoring equipment by the local utility (First Energy) and the system operator (MISO)
2. In both cases, protection systems failed. However, in the Italian case critical section control was basically inadequate to detect the initial failure due to its design, and the load shedding plan failed mostly due to inadequate maintenance of its quite sophisticated protection scheme and to inappropriate setting of power generators protections (both these causes are related, in turn, to multi-jurisdictional property of the generation, transmission and distribution assets), while in the US case most of the blame was put on the inadequate setting of the backup line protection equipment (a much more elementary device than the Italian one).

3.4 Control technologies: a prospective view

In summary, although most ICT infrastructures were reviewed to cope with market liberalisation, recent blackouts pointed out several inadequacies, see previous section 3.4. As discussed, liberalisation is bringing about higher number and more hectic electricity cross border exchanges, while the power grid and its command and control infrastructure have not been substantially updated. New control technologies are emerging (adaptive protection systems, dynamic security assessment, wide area measurement systems). All these systems are inherently based on collecting data in different places, and possibly over an extended period of time, so as to detect an impending malfunction affecting a large portion of the overall system, hence they are inherently based on fast processing and communication techniques.

The unstoppable trend towards a tighter integration among power system monitoring, control and protection, and business systems, as well as towards increased use of open communication channels and off-the-shelf components in those systems, like the TCP/IP protocol and standard operating systems (Windows, Linux, SunOS) is likely to further compound the vulnerability of these systems in the coming years. Large vertically integrated utilities, such as the former EdF and Enel, used to design their own control systems, possibly using proprietary solutions for the ICT infrastructure. As this is now either impossible or impractical in most cases due to sector restructuring, new company policies, obvious advantages of off-the-shelf solutions in terms of cost and interoperability, the vulnerability of emerging solutions for power controls may be further compounded.

In the following section, we will present a brief outline of the emerging control technologies, and then focus, in a conclusive section, on the vulnerabilities this revision process may bring about.

System Protection Schemes

Automated systems like Critical Section Control and the Load Shedding Plan discussed in Section 3.4 pertain to the wide category of the so-called Special or System Protection Schemes (SPS). System Protection, as opposed to Equipment Protection, is designed to counteract system-wide syndromes, rather than protecting specific equipment from large currents and over-voltages.

Quite clearly, SPS are inherently based on measurement sampling over wide portions of the grid. These data are collected and processed in a central place, so as to recognise whether the system inclines towards a dangerous state, and react appropriately. According to the CIGRE` Task Force 38.02.19 [2001] ”*A System Protection Scheme is designed to detect abnormal system conditions and take predetermined, corrective action (other than the isolation of faulted elements) to preserve system integrity and provide acceptable system performance”*. According to [Anderson & Le Reverend, 1996] SPS is *“… a protection scheme that is designed to detect a particular system condition that is known to cause unusual stress to the power system and to take some type of predetermined action to counteract the observed condition in a controlled manner. In some cases, SPSs are designed to detect a system condition that is known to cause instability, overload, or voltage collapse. The action prescribed may require the opening of one or more lines, tripping o generators, ramping of HVDC power transfers, intentional shedding of load, or other measures that will alleviate the problem of concern. Common types of line or apparatus protection are not included in the scope of interest here.”*

Another distinction which is often made in the literature is in between *Event-based* protections and *Response* or *Phenomenon-based* protections schemes [Jonsson, 2003]. The latter are inherently based on observing the system state over a period of time, so as to detect a system-wide perturbation (hence postulate collecting data over that region for that period of time), while the former may be based on triggering after a specific event. Line Protections discussed in 3.2 are typically event-based, although the concept of Event-based protection may also apply to more sophisticated schemes coordinating protections on a local area. In any case, *Event-based* protections react fast, as soon as they detect a triggering condition, like generation rejection or remote load shedding initiated by the tripping of a specific transmission line. *Response-based* systems, like under-frequency or under-voltage load shedding are usually decentralised, hence inherently slower, but more reliable, as they are insensitive to the failure of a single component.

Zima [2002] provides a classification of SPSs according to the disturbance they are designed to cope with:

- *Under-frequency* load shedding devices (UFLS) *“are usually triggered when frequency sinks to the predefined level and/or with a predefined rate of change. … Their action is disconnection of the load in several steps (5 - 20 % each) from the feeders they supervise. However, their effective use is strongly dependent on their careful tuning based on pre-studies, since there is no on-line coordination between them. Another disadvantage is, that they can only react to the under frequency, increase of frequency is not covered by them at all. In some cases the impact of their operation may be negative, since they are not capable of the adaptability to the present situation (e.g. production of distributed/decentralized* *generation varies in time so quite often the distribution voltage level feeders feed the energy back into the network. So they don't appear as loads and their disconnection makes situation even worse)."* This is clearly what happened with the Italian blackout of September 2003.

- *Voltage instability* is coped with a variety of approaches mostly based on identifying the system state against a given model. The grid in the supervised node may be modelled by its Thevenin equivalent and the load by impedance. *"The point of equal impedances (rule known from the basic circuit theory) is then representing a boundary between stable and unstable conditions."*. Other approaches are based on power flow calculations. "*When the system approaches instability, the solution becomes unfeasible due to the singularity of the Jacobian matrix. This provides the basis for a number of indices expressing the proximity to voltage collapse*" [Berizzi et al., 1996]. Zima [2002] further quotes several other approaches based on constraint propagation, continuation power flow, quasi-steady state approximation, model predictive control. Most of these methods were developed in the '90. Some are operational and proved their effectiveness. These include control based on simple stability indices like the one employed in the Italian grid [Corsi et al., 2000].
- *Large Disturbance Rotor Angle Instability (Transient Instability)* is coped with by computation of the equal area criterion, expressing a balance between the accelerating and the decelerating energy. Application on emergency control has been pioneered in the late '90. The angles of the generators are predicted approximately 200 ms ahead. A package based on that principle, intended for on-line use, was developed by Powertech Labs and is now commercially available [Kundur, 2000]. According to Zima [2002], computation times are in the range of 3'-5' for real size grids (300 nodes).
- *Small Disturbance Rotor Angle Instability* is damped in the traditional way by power system stabilisers which modulate the output of each generator. However this requires coordinated and accurate off-line tuning of these controllers, which is the weak point of this approach. Other approaches are based on the use of FACTS devices. Most recent approaches are based on Wide Area Monitoring Systems (WAMS) based on Phasor Measurement Units (PMUs).

According to [CIGRE, 2001] (also quoted by Zima [2002]) the basic requirements about SPS are:

- *Dependability – The certainty that the SPS operates when required, that is, in all cases where emergency controls are required to avoid a collapse.* [7]
- *Security – The certainty that the SPS will not operate when not required, does not apply emergency controls unless they are necessary to avoid a collapse.*
- *Selectivity – The ability to select the correct and minimum amount action to perform the intended function, that is, to avoid using disruptive controls such as load shedding if they are not necessary to avoid a collapse.*
- *Robustness – The ability of the SPS to provide dependability, security and selectivity over the full range of dynamic and steady state operating conditions that it will encounter.*

According to Zima [2002], "*The trend is quite obvious; the most SPSs have been commissioned in the nineties. The degree of complexity is rapidly increasing and the solutions are more and more sophisticated*". He also provides three important statements about the state of the art of SPSs:

- *"All installed SPSs are dedicated solutions for particular power systems. There is no scheme that could be applied to another power system with minimal modifications.*

[7] It is interesting to notice how this source uses Dependability as a synonymous of Reliability as defined according to the Electrical Engineering view (see sections 2.1-2.3).

- *All installed SPSs are either fully or in major part designed and installed by utilities. There is no company that would offer a SPS to utilities as a complete solution ranging from data acquisition to execution of control actions, except ABB.*
- *(…)the costs of the false trips is generally much lower than the cost of failure of the SPS to operate when required. This implies, that even with the risk of malfunction, SPS installation is economically beneficial/profitable.*”

Wide Area Measurement

As discussed in section 2.2, Dynamic Security assessment includes all methods to evaluate the stability of the power system under dynamic conditions. As DSA methods consist of identifying the state of the power system against a complex model whose features may lead to combinatorial explosion, they may be complemented by any coordinated approach to augmenting the *observability* of the system by taking an additional number of measurements (Wide Area Measurement). Most recent approaches to WAM are based on phasor measurement units (PMUs): These units provide in real-time GPS-synchronised measurements of voltage and current phasors. The technology allows a faster and accurate calculation of active and reactive power flows, based on voltage and current phasor measurement, which permits also to carry out modal analysis and fault detection and recording. At the same time it permits, through GPS-synchronisation, the comparison of absolute angles and the evaluation of relative angles, which puts in evidence stressed corridors, voltage instability and collapse margins, frequency instabilities due to network separations, angle instability risks between both network areas and single generators with respect to the rest of the grid, as represented by its Thevenin equivalent. From a physical viewpoint, phase measurements give a way to estimate whether a network area or a single generator is able to deliver its power output to the rest of the grid. When this does no longer happen (usually because of a short circuit reducing coupling between a generator and the resisting torque of the load) the generator will start accelerating until it is damaged (more realistically, until a feedback controller reduces its speed), while other generators, having to face an increased load, will conversely reduce speed.

Comprehensive monitoring of the grid behaviour over time would require instrumentation of all its topological nodes. In practice, to reduce cost both of the measurements and of communications, it is required to minimise the number of PMUs. This may be achieved by selecting a set of strategically placed monitoring buses. Further measurements are then added until the time performance of the monitoring system does no longer improve. This way a highly reliable DSA system can be built [Kamwa and Grondin, 2002]. Their method applies fuzzy reasoning and Fast Fourier transforms to decide at a prescribed time whether a contingency is permanently stable: this way, it is able to single out 77% and 91% of all stable cases, respectively within 1 sec. and 2 sec. of the contingency. [Kamwa et al., 2003] show that the selected phase measurements monitor the behaviour of specific portions of the grid with respect to the system’s center of inertia. These portions comprise a group of generators which will exhibit a similar behaviour, because they are connected to the rest of the grid by the same lines, and may be represented by a single equivalent machine[Kamwa et al., 2003], [Jonsson, 2003].

The above performance means that, although Wide Area Measurements were first introduced in power systems as inputs for state estimation, they can be used to implement fast feed back control schemes [Bose et al., 2004]. Then a crucial point becomes to compute the delay involved by different communication links. Nadhuvathumparambil et al. [2002] show that this is composed of three components:

- the fixed delay associated to data sampling and computation;
- the link propagation delay;
- the ratio between the amount of data transmitted and the data rate of the link.

Under the realistic assumption of using 10-12 PMUs, 4 bytes per measurements, and 10 input status lues (each 2 bytes in length), the fixed delay would amount to 75 ms. For distances between PMUs in the range of 200-300 km, the authors show that the overall delay would be in the range of 100-150 msec for fiber optic cables and digital microwaves, 150-350 with power line communication through the grid lines, 200-300 using telephone lines, and 500-700 for satellite links. The paper also introduces the IEEE 1344 data format to achieve interoperability among PMUs.

A key point, however, should be noted: with the current state of communications, if WAMs were to be used in a feedback control system, the control logic could not stand far away than 200-300 km. from the PMUs. This is fairly different from the current organisation of control in most European countries, where overall control is managed by a limited number of control centres, at a distance which often exceeds 500 km from the remote terminal units. Hence, adoption of WAM-based control would mean to establish an intermediate control level which may not easily fit into the current control strategy and organisation.

In conclusion, WAMs can be used:

- as monitoring systems, and in that case the key issue is of course how to interface the systems to the human operator so as to make possible a fast appropriate reaction (as discussed, after collapse of a major element of the grid, reaction times should be contained within a few minutes only);
- in control loops: in this case however, several issues remain open (the control algorithm itself, reliability of communication etc.) before they can be widely adopted.

Adaptive relaying

The performances mentioned in the previous section should be compared with the 3rd zone time delays in conventional protection systems mentioned in chapter 3.2 (0.4 to 1 sec.). In principle, the faster communication links would allow a control system to pre-empt back-up relays of conventional protection systems. Actually, off-the-shelf digital protections settings may be changed on-line either by a local or a remote controller. As discussed in 3.2, all relay settings are a compromise between security and adequacy, i.e. between economy and performance. The principle of adaptive relaying is to change adaptively the settings of directional, distance, frequency and other relays as the system configuration changes. A quick overview of modern trends in power system protections is given by Wilks [2002], where adaptive relaying is defined, according to the classical definition by Phadke and Horowitz [1990] as *'a protective philosophy which permits and seeks to make adjustments in various protection functions automatically in order to make them more attuned to prevailing power system conditions.'* A more extended bibliography on adaptive relaying, with a few practical examples, is provided by [Sidhu and Rosas, 2003]. Applications range from changing relay settings, to adapting to a different source impedance configuration, to more sophisticated schemes of adaptive protection using neural networks. One of the most debated subjects appears how to realise adaptive distance protection, so as to adapt to changing system conditions. However, most schemes appear to be based on adaptive algorithms built in the protection's microprocessor, so as to achieve adaptation by measuring system conditions in the protection boundary, rather than relying on a local or wide area scheme, where settings would be changed according to prevailing system conditions in a wider region.

Conclusion

The present overview outlines how the growing complexity of electrical systems requires robust control strategies and innovative/new SCADA. Operational control is moving towards more sophisticated control strategies and higher speed, more intelligent local control and protection. However, the complexity of the infrastructure to be controlled in the context of progressive establishment of a European energy market implies a number of outstanding challenges, which were summarized as such in a recent workshop on the emerging security challenges affecting power systems [RAmI, 2005]:

- *Need to establish confidence in performances that may be reached with new technologies such Wide-Area Monitoring:* as discussed in the previous section, several issues specifically concerning technology performance are to be addressed, e.g. criteria for PMU positioning, reliability of their synchronization process, performances of the algorithms, etc.
- *The human factor:* one key factor for the blackouts was that current controls rely too much on the role of humans, who are fallible and cannot cope with real time constraints. On the other hand, humans cannot be removed from the loop, because they are extremely good at dealing with unforeseen situations such as those that might arise from malicious attacks. Humans should play a more strategic role in supervisory control, while enhancing wherever possible fast automated response at a local level.
- *Need to exploit the potential of new technologies for local protection and control:* the potential of innovative technologies for smart local control at the substation level, like adaptive relaying, need to be fully exploited. Their appropriate integration into a multi-level/multi-area hierarchical control structure must be investigated.
- *Need for non-intrusive technology migration paths:* new technologies should come with an evolutionary approach to upgrade existing legacy control systems, so as to resolve concerns related to communication, resilience, integration of new technologies in the control loop. This upgrade is made even more complex because legacy systems are full of bugs, often they were developed without any methodology, and their development and support tools are outdated. In that context, it is apparent the importance of methodologies to master the life cycle of control systems, discussed in section 2.3.
- *Need to address weak areas of the EU grid, especially cross-border ones:* much work has to be done regarding decomposition and allocation of control functions especially cross-border, e.g. Switzerland/France/Italy and France/Spain. Moreover, the legal framework among neighbouring countries is very different; hence it is difficult to mandate this task to somebody.
- *Ensure resilience of the telecom infrastructure underlying SCADA:* next generation systems will also require a high performance, secure and high quality service infrastructure, also to support flexibility, restore systems and recover data. In that context, cyber vulnerability is becoming a major challenge. Distributed control and protection systems, whilst providing opportunities for enhanced control and efficiency, also increase the exposure of the power

infrastructure to accidental and malicious failures. The fading of boundaries and convergence of corporate and control networks also increase the cyber vulnerability of control systems.

3.5 Resilience of the ICT infrastructure: the role of standards

This final chapter will deepen on the issue of resilience of ICT introduced in the previous chapter. Specifically, we will analyse the *role of standard*s for communication in that perspective: in fact, vulnerabilities due to design and technology flaws may be exploited thanks to the lack of appropriate regulations. This threat was perceived by the industry both in the specific sector of power system controls and in the process sector at large. However, there is a time gap between the availability of standards and their application. The current efforts to consider security in communication standards are too recent for being sure about their effectiveness. In the meantime the power sector will continue deploying control systems. This opens a negative window of opportunity of several years for cyber attacks and failures.

Standards are a key driver in the development of engineering systems in general, and of the power sector in particular. Standards, which can impose a certification scheme, constrain the technical choices, or harmonize by promoting their voluntary adoption. With reference to ICS and specifically to security, standards will be fundamental for the creation of a market and for supporting the procurement process. As a consequence, the design and implementation of security countermeasures will be facilitated, best available practice can be applied in a consistent way, and the risks across the infrastructure can be reduced in a uniform way.

But, what is the current status of ICT security related standards? Reality is that the production of standards is at its early stages. Acknowledgement of their importance is rather new – less that a decade old; and awareness of their urgent need if more recent.

The situation is challenging, and by all accounts will continue to be so for the next decade – if not more. Industry is already waiting for standards that will not be ready in the next coming years. In the meantime information and communication technologies are being deployed with an ad-hoc approach to security, based on the restricted knowledge of each company.

There is therefore the risk that standards will arrive too late: when some important accidents will have happened, and when non-standard and incompatible solutions will be in use. As information and communication systems are at the core of the interconnections among the different actors of the electric power sector, the delay in the availability of effective standards is by itself another vulnerability issue: the near future will see a great window of opportunity for incidents related to intentional exploitation of this vulnerability.

This deficiency has to be dealt with immediately, as any further postponement of clear positions by industry and regulators can aggravate the security conditions. The answer to this situation can take the form of an intermediate set of guidelines and best-practices to be applied in the transitional period until appropriate standards will be complete. This is the approach in North America, with the leadership of institutions such as the North America Electric Reliability Council (NERC) and the USA’s National Institute of Standards and Technology (NIST). Similar initiatives would be greatly desirable in Europe.

A further factor that will have to be taken into account is the convergence with telecommunications and particularly the work on Internet. Although the electric applications run on top of the communication layers provided, the evolution of the latter will significantly affect the functionality and security of the others. Not the least, some other vendors and communities might come from the telecommunications and computing networks sector, offering their security solutions and constraining the electric power sector choices.

Power Sector Standards and Recommended Practices

The necessity for the consideration of information and network security in the electric power sector standards was acknowledged in the late 90's only. The proprietary and isolated nature of the ICS equipment up to those years seemed to require no special provision.

The International Electrotechnical Commission (IEC) is the leading international body for electrical, electronic and related technologies. Its Technical Committee 57 "Power Systems Management and Associated Information Exchange" issued the Technical Report TR62210 in May 2003 discussing the security aspects related to the computerised supervision, control, metering and protection in electrical utilities. TC57 recognizes in its Strategic Policy Statement (IEC, 2003) that "The fast development of information technology (IT) and communication technology has impact on the work of TC57". A key point of the strategy is to open proprietary structures by standardization of data exchange interfaces among IT systems and software applications".

The committee collaborates with other organisations making important developments with respect to SCADA security, such as the American Gas Association (AGA), the Instrumentation, Systems and Automation Society (ISA) and NIST. It is composed of a relevant set of working groups, among them: telecontrol protocols, distribution automation, substation communication, application program interface for Energy Management Systems, communication for deregulated energy markets, interfaces for distribution management systems, interoperability, and especially the Working Group 15 data and communication security, launched in October 1999. The dates show that the intervention was arriving late with respect to the actual use of insecure remote access equipment in the field installations.

TR 62210 illustrates the risks associated with the typical IEC communication protocols, examining some threats, vulnerabilities and potential consequences of electronic intrusions. The document also considers some actions and countermeasures that can be applied, and presents a first attempt to analyze the risks with a cause-consequence diagram.

A first lecture of the IEC's Technical Report (Dondossola, 2004) puts on view some unusual elements for Technical Committees dealing with "computerised supervision, control, metering, and protection systems in electrical utilities":

- It is recognised that information and communication systems security involves the "corporate security policy", which should be the departure point of the so called "Normal corporate security process". But that security policy is not part of the customary practice of electric power companies. How many European companies do have an explicit information security policy? And if yes, which are the references for the industrial control and communications sections?

- It is recognised the importance to create common vocabulary, as shared notions are the basis for standards. Threats, vulnerabilities, information security etc. are not yet stabilised notions.

- It is recognised that vulnerabilities and threats have to be analysed with reference to the consequences that might be produced. Some of the consequences suggested point to the broad set of elements that need to be examined: loss of revenue due to increased competition or contractual disputes, reduced profitability due to cash flow disturbances, manipulation of production and consumption data that leads to erroneous forecasts, artificial change in stock value, asset destruction or degradation, etc. In addition it is evident that most of these topics fall outside the typical analytic space of engineers, indicating that assessing these consequences will not be easy, and will demand suitable methodologies and the participation of a considerable staff.

- It is recognised that the network topology interconnects all actors of the electric power system, technical and market-related. The suggested list of stakeholders is ample: obviously generation, transmission and distribution companies, but also data aggregators (business entities that for instance process and combine metering data), meter service providers, electricity suppliers without installations (that operate in the electricity wholesale market), risk management market participants (that sell, trade, broker or operate with derivatives in the market), and finally the end customers (who expect not just the supply of energy, but also information services related to the technical operations, the commercial relations and the market). This broad set of actors also point to the potential difficulty of the security assessment.
- The report suggest the employment of a methodology for the assessment (i.e. consequence diagrams), that requires the identification of all relevant stakeholders, the business processes that concern them, the consequences that can adversely affect those processes, and the events that might provoke those consequences. This will serve for ascertaining the threats and the vulnerabilities that are of primary importance. If such assessments are to be accepted as necessary, it is apparent that much more research in the field and training of personnel will be required.
- The report finally links the identified relevant threats to the specification of the protocols developed by the Technical Committee 57, and especially the Telecontrol Application Service Element No. 2 (known as TASE.2), and the IEC 61850 and IEC 61334 series (respectively devoted to communication networks and systems in substations, and distribution automation using distribution line carrier systems). It is proposed to apply the standard ISO 15408 (known as Common Criteria, discussed later in this chapter), for the generation of Targets of Evaluation (TOE) and Protection Profiles (PP) for the protocols. A vast work can be foreseen in the interplay between the specificity of each installation (and consequently their own security risk) and the genericity of TOE and PP. The needed standards will not be available in a short period.

The International Council on Large Electric Systems (CIGRE') convened in 2003 the Joint Working Group D2/B3/C3-01, with participation of the Study Committees D2 (Information Systems and Telecommunication), B3 (Substations) and C3 (System Environmental Performance). Its objective is explicitly the security of the ICS of the electric power systems. The working group is producing a series of papers that will undoubtedly serve for raising awareness in the sector. The first two papers have been published in the journal Electra (CIGRE, 2005a; CIGRE, 2005b). The intention is to present a series of reflections and suggestions of immediate actions that could help in bettering the level of ICS security ad the development of proper security policies.

In North America, NERC (North American Electric Reliability Council) has organised a Cyber Security Urgent Action, resulting in some guidelines, compliance audits, and activities such as workshops for raising awareness. In 1998 the USA's Department of Energy assigned to NERC the role of co-ordinator of critical infrastructure protection activities reference point for the electric power sector, including cyber security. It was created the CIPC (Critical Infrastructure Protection Committee) that develops and maintains capabilities to respond to security threats and incidents, and supports the production of standards and guidelines. In June 2002, NERC issued the "Security Guidelines for the Electricity Sector" that cover physical and cyber security, along with emergency plans and business continuity. The approaches and practices recommended are generic, and no indications of particular methodologies are given. In any case, the guidelines are useful for disseminating common requirements and could act as a basis for further developments.

NERC's Cyber Security Urgent Action was set with the purpose to reduce the risks from any compromise of critical cyber assets. A first standard (known as Urgent Action Cyber Security Standard 1200) was issued in August 2003. It is applicable to control centres only and aimed at self-certification. The Draft 2 of the last Cyber Security Standards proposed by the NERC Action (CIP-002-1 through CIP-009-1, formerly known as Urgent Action Cyber Security Standard 1300) was issued in August 2003 and is currently under review by the drafting team. It is expected to be finished by mid 2005 and applies to control centres, power plants – except nuclear– and substations and lists several tasks that are deemed essential for cybersecurity, ranging from security management controls, to the identification and definition of critical assets, controls, personnel, and functions such as training, systems security management, incident response and recovery plans. But it doesn't consider control system protocols.

The standard presents detailed metrics. Its importance resides more in its specification of basic requirements and measures, and the definition of compliance monitoring processes, levels on on-compliance and sanctions. This is a language easily understandable by industry and demonstrates a significant commitment. This type of approach, although its results will always be far from comprehensive, gives an important indication to all players in industry and regulatory bodies: the recommendation we can derive is that the problem is serious, basic solutions are urgently needed, compliance and enforcement are a must.

In parallel NERC manages the ES-ISAC (Electricity Sector Information Sharing and Analysis Center), for the exchange of information on critical risks in the electric power sector. In particular two indexes have been developed for indicating the threat levels as well as for indicating the possibilities of physical and cyber attacks. These instruments are very helpful for creating alertness on the situation, but also a general awareness on the risks.

Other Industrial Control Initiatives

In parallel, IEEE has been producing some standards, such P1547 for "Interconnecting distributed resources with Electric Power Systems", 1525 for substation automation, and 1379 for substation IED communication. The IEEE Substations Committee has the task force C0 TF1 that deals with Substation Data Security. An open question remains on the multiplicity of efforts for a sector that needs promptly answers.

There are related activities in other industrial sectors that are germane for electric power. In the Instrumentation, Systems and Automation Society (ISA), the committee SP99 looks after control system security. CIGRE takes part in this initiative. ISA has a standard under development that will be issued in the coming years, with a muti-industry focus. Part 1 that aims at the consolidation of models, definitions and terminology will be ready by the end of 2005. Part 2, dealing with security programs and the analysis of risks and vulnerability will be presented in draft forms in the following months. Part 3 (on Security Programs) and 4 (on Security requirements and controls) will only begin their development in the future. There is of course no guarantee that the adopted terminology and methodology by ISA, although coherent and efficacious in their context, will not enter into conflict with other initiatives.

The American Petroleum Institute has been working on cyber security guidelines documents and API 1164 is the first (published in 2004) dealing with SCADA security best practice. Its goal is to provide an easy to follow and rapid guide to industrial companies mainly in the pipeline sector – but their applicability is broader. There are no plans for third party certification or requirements on self-certification. Although incomplete and not very sophisticated from the security viewpoint (for instance in the consideration of authentication and access control, links to security policies, etc.), it provides ready applicable and sound recommendations. It is therefore a straightforward, practical and undemanding effort that, if applied by industry, can have immediate effects. As a provisional action while waiting for more thorough measures, it is a lesson to learn by the European electric power sector.

The American Gas Association (AGA) initiated quite early some initiatives in the context of infrastructure security. Already in 1988 they had the first discussion in the use of encryption protocols to protect the gas sector communications and the SCADA systems. The first technical proposals by the Gas Technology Institute (GTI) received scarce attention, due to the lack of awareness on the risks. Only after the September 11th 2001 events there was some consciousness that specific safeguards were required. The work is conducted by a dedicated working group that has delivered the standard report AGA 12 "Cryptographic Protection of SCADA Communications" (Draft 4), issued in November 2004. Although the work is limited to the encryption of communications, the working group pointed to the beginning to generic results targeting several industries: gas, electric, water, wastewater and pipeline real-time control systems. It should be considered that encryption is a valuable solution, but it is first needed to understand the problem: the security risks.

NIST has released in April 2004 a System Protection Profile for Industrial Control. This has been developed in the context of the Process Control Security Requirements Forum (PCSRF). The specification follows the Common Criteria, as a starting point for the specification of security requirements. The document extends the typical elements of a Protection Profile (PP) to broaden security controls to non-technical procedures and management functions. The PP is generic to all kinds of industrial control, focusing in the subset of elements that are applicable to all implementations. Very importantly, NIST highlights that security functions should respond to risk analyses and dedicated assessments, and that these assessments should be applied to new designs, but also for retrofits and upgrades.

General-Purpose Standards

There are two general standards that set the reference framework for all initiatives in information security: ISO 17799, the Code of practice for information security management, and the already mentioned ISO 15408, the Common Criteria. Both standards provide guidance to security management and the specification of security requirements for products, respectively. But they don't demand the application of specific methodologies or technical architectures.

ISO 17799, derived from the British Standard 7799 and produced by the ISO/IEC Joint Technical Committee 1, Subcommittee SC 27, in December 2000, presents a starting point for developing organization specific guidance arrangements. It is a "comprehensive set of controls comprising best practices in information security”, and comprises a code of practice and a specification for an information security management system.

A corporation applying it will have to perform a risk assessment, prepare its security resources, and prepare the needed elements for certification and compliance. These will include the corporate security policy, and the functional and assurance requirements that have to be implemented. The standard provides a generic list of these requirements at a high level, independently from specific technologies. A fundamental point is the provision of appropriate security policies. A policy should set the direction for action and the commitment of the company to information security. Remaining at the management level, the application of this standard to industrial installations, mainly one with potential critical consequences, seem to merit a review, or at least a complement with particular considerations on, for instance, timing issues related to control applications.

As a single reference point, ISO 17799 is important for providing a common view on administrative and industrial information and communication systems. If companies across an industrial sector would apply it, the creation of a trusted environment will be fostered.

The Common Criteria are the result of long developments in the USA, Canada and European countries (the Netherlands, France, Germany, United Kingdom), and aimed at supporting the specification of products with security requirements. First published in 1996, its second version was adopted by ISO as standard 15408 in 1998. The requirements to be defined are functional requirements, those related to desired security behaviours, and assurance requirements, which are the basis for gaining confidence that the claimed security measures are effective and implemented correctly. The standard gives the possibility to select among seven evaluation assurance levels, which can be used for grouping components, or provide retrofit compatibility with existing products (first 4 levels), or develop specialised components.

This standard supports purchasers of products in the definition and formulation of the requirements they necessitate; vendors or developers in the specification of their products, and third party evaluators in the verification and validation of products. In this way, the whole procurement process is assisted with common terminology and procedures.

It is understandable that several approaches to the security of industrial control have taken the Common Criteria as reference. However it should be considered that this standard, although technically important, has not been heavily applied in the real world. Verifying technical products against a standard that comprises functional and assurance procedures is very costly. Some significant criticisms are that the evaluations don’t seem to add value while entail notable costs, that it doesn’t have a noteworthy impact on the reduction of vulnerabilities, that the engineering efforts could be better employed in other technical tasks related to security.

As a consequence, we can say that the Common Criteria might mature into a useful framework for the development and procurements of security devices. Nevertheless, it will take time and will be dependent on the evolution of the standard in other fields. In addition, the more immediate needs of the electric power sector seem to lie in the system evaluation area – and this is not currently supported by the Common Criteria. These will have to evolve, incorporating new assurance requirements.

3.6 Bibliography

[AEEG, 2003] *Sintesi dell’Istruttoria Conoscitiva sulle Interruzioni del Servizio Elettrico del 26*

Giugno 2003, , Autorità per l'energia elettrica e il gas, 6 dicembre 2003
http://www.autorita.energia.it/com_stampa/index.htm

[AEEG, 2004] *Resoconto dell'Attività Conoscitiva in Ordine alla Interruzione del Servizio Elettrico Verificatasi il Giorno 28 Settembre 2003*, Autorità per l'energia elettrica e il gas, 9 giugno 2004
http://www.autorita.energia.it/com_stampa/index.htm

[Anderson & Le Reverend, 1996]: *Industry Experience with Special Protection Schemes*, P. M. Anderson, B. K. LeReverend, IEEE Transactions on Power Systems, Vol. 11, No. 3, August 1996.

[Berizzi et al., 1996]: *System-Area Operating Margin Assessment and Security Enhancement Against Voltage Collapse*, A. Berizzi, P. Bresesti, P. Marannino, G. P. Granelli, M. Montagna, IEEE Transactions on Power Systems, Vol. 11, No. 3, August 1996.

[Bose et al., 2004] *A Dynamic Optimisation Approach for Wide-Area Control of Transient Phenomena*, A. Bose, S. Bruno, M. De Benedictis, M. La Scala, CIGRÈ General Meeting, Paris, August 29 - September 3, 2004.

[CIGRE` Task Force 38.02.19, 2001] *System Protection Schemes in Power Networks*, June 2001.

[CIGRE, 2004] *Managing information security in an electric utility*, Joint Working Group D2-B3-C2.01, Electra, n. 216, October 2004.

[CIGRE, 2005] *Cybersecurity considerations in Power System Operations*, Joint Working Group D2-B3-C2.01, Electra, n. 218, February 2005.

[Dondossola et al., 2004)] *Emerging standards and methodological issues for the security analysis of the Power System information infrastructures*, G. Dondossola, M. Masera and O. Lamquet, CRIS 2004 Conference: Securing critical infrastructures, Grenoble 25-27 October, 2004.

[Corsi et al., 2000]: *A Simple Real-Time And On-Line Voltage Stability Index Under Test In Italian Secondary Volage Regulation*, S. Corsi, M. Pozzi, U. Bazzi, M. Mocenigo, P. Marannino CIGRE, 38-115, Session 2000.

[CRE AEEG, 2004] *The joint conclusions of the inquiry of the Italian and French regulatory authorities on the international causes of the September black out.* Press release dated 04/23/04
http://www.cre.fr/uk/ressources/communiquesdepresse/communiquesdepresse_consultation.jsp?idDoc=1864

[Eurelectric, 2004] *Power Outages in 2003*, Task force Power Outages, June 2004
http://public.eurelectric.org/Content/Default.asp?PageID=173

[GRTN 2004] *Guida Tecnica n° INSIX 1006 Rev.00 - Piani di Difesa del Sistema Elettrico*, GRTN-Ingegneria dei Sistemi.

[IEC, 2003] *Power system control and associated communications – Data and communication* *security*, Technical Report TR 62210, May 2003. Available from http://www.iec.ch/

[Jonsson, 2003] *Protection Schemes to Mitigate Major Power Systems Breakdowns*, Dissertation Thesis, M. Jonsson, Göteborg, 2003.

[Kamwa & Grondin, 2002] *PMU Configuration for System Dynamic Performance Measurement in Large Multiarea Power systems*, I. Kamwa and R. Grondin, IEEE Transactions on Power Systems, vol 17, No. 2, May 2003.

[Kamwa et al., 2003] *Rapid Stability Assessment of Extreme Contingencies Based on Wide-Area Severity Indices*, I. Kamwa, R. Grondin, A. Henniche, G. Trudel and L.Riverin, CIGRE'/IEEE Int. Symposium on Quality and Security of Electric Power Delivery Systems, Montreal, 2003.

[Kundur et al., 2000]: *Techniques For On-Line Transient Stability Assessment And Control*, P. Kundur, G. K. Morison, L. Wang, IEEE Power Engineering Society Winter Meeting, 2000.

[Russel Mason] *The Art & Science of Protecting Relaying*, C. Russell Mason, General Electric Co. – GE Consumer and Industrial – Electrical Distribution. http://www.geindustrial.com/pm/notes/artsci/

[Naduvathuparambil et al., 2002] *Communication Delays in Wide Area Measurement Systems*, B. Naduvathuparambil, M.C. Valenti, and A. Feliachi, Proc. Southeastern Symp. on System Theory, pp. 118-122, Huntsville, AL, March 18-19, 2002.

[Phadke and Horowitz, 1990] *Adaptive Relaying*, A.G. Phadke and S.H. Horowitz, IEEE Computer Applications in Power , vol. 3, issue 3, July 1990, pp 47-51.

[RAmI, 2005] *The future of ICT for power systems: emerging security challenges*, Report of the Consultation Workshop held in Brussels on February 3-4, 2005. https://rami.jrc.it/workshop_05/Report-ICT-for-Power-Systems.pdf

[Sidhu and Rosas, 2003] *Computer-based Protection Course – Adaptive Relaying*, T.S. Sidhu and G. Rosas, The university of Western Ontario, December 2003.

[Stefanini, 2005] *Electric System vulnerabilities: lessons from recent blackouts and the role of ICT*, A. Stefanini, JRC Report EUR 21551 EN, February 2005.

[UCTE, 2003] *UCTE Operation Handbook – Policy 3, Appendix 1*, http://www.ucte.org/ohb/cur_status.asp.

[US-Canada, 2004] *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, U.S.-Canada Power System Outage Task Force, April 5, 2004, http://www.nerc.com/~filez/blackout.html

[Wilks, 2002] *Developments in Power System Protection*, J. Wilks, Annual Conf. of Electric Energy Assoc. of Australia, Canberra ACT, 9-10 August 2002

[Zima 2002] *Special Protection Schemes in Electric Power Systems – literature survey*, M. Zima, ETH Zürich, June 2002.

4 Conclusions

This report has provided an overview of the crucial factors involved in most recent huge blackouts, and a first analysis of the reasons why existing weaknesses in power system controls could result into such dramatic outcomes. Also, it has outlined the gap between the maturity of innovative control technologies, and the limitation of present day methodologies for designing and validating distributed control systems. If this gap is not reduced, there is little chance that the new advanced control schemes will become reality. Awareness of this challenge was the main motivation for a recent workshop on the subject [RAmI, 2005], aimed at fostering discussion among stakeholders and the research community on the role of pervasive information & communication technologies applied to power systems. The conclusions of this report are largely based on the outcomes of this workshop.

One has to consider that the organizational and technological evolution of electric power systems occurs within a broader landscape. The drivers shaping the space where the electric power infrastructure develops are:

- technology is becoming more and more the fabric of our society;
- stronger integration of control and communication, more homogeneous control and communication protocols;
- fading of boundaries, convergence of business and control functions in corporate networks;
- all services to be delivered through similar channels and interdependent among them.

More specifically, all new power system controls are likely to make growing use of open ICT infrastructures and off-the-shelf hardware and software components. The market brings about growing standardisation of ICT components and services:

- almost all off-the-shelf remote control systems use the IP protocol;
- the market provides standard remote control solutions to the whole process sector independent from the specific domain (electric power, oil and gas, chemicals etc.);
- local area off-the-shelf solutions (eg Bluetooth, WiFi) may also be very vulnerable:
- the adoption of off-the-shelf standard solutions and transformation of ICT infrastructures in multi-jurisdictional systems (open to a user community extended across national boundaries) largely compounds their vulnerability.

In summary, the main challenges and concerns that review of power systems control is bringing about appear to be related to:

1. **The applicability and the impact of advanced control and communication technologies on the overall architecture of power control systems**: although there is consensus about the key role that emerging technologies like WAMS and innovative protection schemes in the future controls of electrical networks, several issues remain to be resolved concerning integration with legacy systems, better and faster communications to support flexibility and quality of service, resilience against security threats, and the methods to prove and verify new control applications.
2. **The need to cope with more threats and vulnerabilities**: Designers have to cope with more uncertainty in a competitive environment, which causes that considerable amount of knowledge and data is not shared. Moreover, we have to face new types of threats (e.g. malicious attacks) and vulnerabilities (e.g. uncertainty about data and components behaviours) that are hard to model. Cyber vulnerability is becoming a major challenge.

Distributed control and protection systems connected to global supervision networks by means of Internet technologies, whilst providing opportunities for enhanced control and efficiency, also increase the exposure of the power infrastructure to accidental and malicious failures. We need to identify and monitor attacks against control systems as well as to integrate e-attacks into risk assessment.

3. **The move from dedicated to off-the-shelf systems**: the use of COTS will increase the likelihood of malfunctions and unexpected behaviours of components in the control loop.
4. **The need to cope with distributed generation and renewables**: the amount of distributed generation will increase and the mix among power sources will spread. This is a further factor requiring more flexible and distributed future controls.

In the current situation, where the system can hardly be strengthened by making recourse to physical measures (it is rather hard to build more transmission lines, or to further decentralise power generation due to their growing environmental impact). As it is not reasonable nor envisageable to keep a centralised model of power system expansion in order to cope with demand growth, there is an absolute need for distributed intelligence, that would ultimately reduce the growing complexity of the system. In turn, this requires robust control strategies and innovative/new SCADA. Operational control should move towards higher speed, more intelligent local control and protection. We need to make the system more ductile and self-reconfigurable. We need to decentralise and distribute intelligence (distributed state estimators, distributed generators, adaptive architecture, agent-based estimation). We need to capture, reuse and correlate knowledge and diversity of information, which also involves using different lines of reasoning. More run-time checking, verification and data analysis shall help understanding how to distribute intelligence and enhance controllability. On the other hand, this transition towards innovative control strategies and systems needs to be smooth and evolutionary, so as to take into account the legacy of existing control architectures and currently deployed systems.

A further facet of the above concerns the integration of heterogeneous simulation tools (e.g. dynamic security assessment; discrete runtime models of control& communication) into transmission and distribution grid operation, so as to progress towards *understanding how ICT interact with electrical grids*. This will also allow the development of more sophisticated control strategies, able to adapt to changing requirements, and anticipate threats, based on symptoms and real time indicators.

Also, there is a need to establish confidence in performances that may be reached with new technologies such as WAMS: (e.g. technology performance, criteria for PMU positioning performances of the algorithms, etc.).

This scenario involves a number of purely <u>methodological issues</u> which can be summarized in the following list:

- *Trade-offs of using formal methods:* present day design methodologies relying on formal methods appear too cumbersome and complex to be useful in the design of very large systems. Also, the complexity of power systems is such that the use of heuristic methods is often unavoidable.
- *Need for non-intrusive technology migration paths:* new technologies should come with an evolutionary approach to upgrade existing legacy control systems, so as to resolve concerns related to communication, resilience, ways to integrate new technologies in the control loop. These issues appear to require a joint effort of stakeholders (transmission system operators, utilities) and technology providers.
- *Ensure resilience of the telecom infrastructure underlying SCADA:* next generation systems

will also require a high performance, secure and high quality service infrastructure, also to support flexibility, restore systems and recover data.

- *Identification and modelling:* the immediate challenges for the research and industrial communities are: identifying first key vulnerabilities and controls, followed by models and measurements and development of methodologies and tools. The problem of interplay among infrastructures must be solved, which might benefit from the application of complex systems principles, and complexity theories might help to improve controllability and self-healing. In addition, new methods for testing and reviews must be found.
- *Assessment of vulnerabilities, threats and risk*: The subject is new for power systems and pressing because installations of many ICT systems are being made today without a thorough consideration of the security implications. It is not clear which could be the appropriate (feasible, affordable, efficient) ways for identifying and analysing vulnerabilities and threats, and therefore to evaluate the cyber risks to which it is subject the electricity system, in a context where boundaries are fading (between control & communication, business & control etc.).

Furthermore, the above scenario is made more complex by a number of issues having mostly a political and socio-economic nature. Among them we must mention:

- *How to deal with legacy systems:* Legacy systems are full of bugs, often they were developed without any methodology, and their development and support tools are outdated. However, the cost of their replacement is very high and industry does not have a very strong incentive to proceed with this replacement.
- The cost of security: same predicament applies to the other challenges discussed (e.g. use of COTS, uncertainty, emerging vulnerabilities). The cost of security is high and it is not clear to which extent society is prepared to bear it.[8] There is a need to accurately assess the benefits of security investment in the power sector.
- *The human factor:* one aspect of current controls is that they rely too much on the role of humans, who are fallible and cannot cope with real time constraints as well as stressful situations. Are we prepared to remove humans from the loop? On the other hand, humans are extremely good at dealing with unforeseen situations such as those that might arise from malicious attacks. We must understand how to use local control & local intelligence for global control, at a higher system level, so as to provide different and informative views of the same system. This will allow assigning to humans a more strategic role in supervisory control, while enhancing wherever possible fast automated response at al local level.
- *Need to address weak areas of the EU grid, especially cross-border ones:* much work has to be done regarding decomposition and allocation of control functions especially cross-border, e.g. Switzerland/France/Italy and France/Spain: there is a need for more R&D on decomposition and allocation of security control capabilities in particular in the boundaries of networks, and more algorithms for data exchange/sharing across boundaries. However, the legal framework among neighbouring countries is very different; hence it is difficult to mandate this task to somebody. Concerning security of supply, there is a 'grey area' between the EU and the member states.
- *How to overcome the economically-biased control:* system security and adequacy is a public good. Access to services must be granted on an equal basis, also to peripheral and isolated

[8] Several authors argue that the society cannot cope with the cost of keeping the current security levels of power systems (see Amin, [2005] for the current debate on this issue in the USA).

areas. In view of this, control policies cannot be purely based on economic criteria, even in a competitive market.

- *Risks associated to the spread of monoculture:* stronger integration between control & communication, fading of boundaries and convergence of corporate and control networks increase the cyber vulnerability of control systems. A way ahead in that respect may be the usage of transparent "honey nets" able to capture intruders and classify attack patterns against SCADA and control systems.
- *Role of standards:* vulnerabilities due to design and technology flaws may be exploited thanks to the lack of appropriate regulations. But there is a time gap between the availability of standards and their application. The current efforts to consider security in EPS-related standards are too recent for being sure about their effectiveness. In the meantime industry will continue deploying cyber systems. This opens a negative window of opportunity of several years for cyber attacks and failures. There is an urgent need to act for overcoming this situation, and R&D should support.
- *Competence and proper training are required.* Personnel are frequently not sufficiently qualified to cope with the more critical events, especially when dealing with diagnosis and recovery actions in emergency situations. There is a need to enforce continuous training, even by law.

In conclusion, *Security must be seen as a systemic property:* the top challenge is to understand and accept the risk, in particular for interconnected infrastructures. Security cannot be ensured by local measures; it must be taken into account in all phases of the life cycle of a system, from requirement analysis to design, runtime control implementation, verification and testing, and must apply to all system components.

4.1 Bibliography

[Amin, 2005]: *Powering the 21st century: we can –and must – modernize the grid.* M. Amin, IEEE Spectrum, April 2005.

[RAmI, 2005] *The future of ICT for power systems: emerging security challenges*, Report of the Consultation Workshop held in Brussels on February 3-4, 2005.
https://rami.jrc.it/workshop_05/Report-ICT-for-Power-Systems.pdf

Mission

The mission of the Institute of the Protection and Security of the Citizen of the Joint Research Centre is to provide research-based, system-oriented support to EU policies so as to protect the citizen. The main application areas are cyber-security and the fight against fraud; natural, technological and economic risks; humanitarian security, non-proliferation and nuclear safeguards. The Institute will continue to maintain and develop its expertise in information, communication, space and engineering technologies in support of its mission.

EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre