The International Emergency Management Society
9th Annual Conference Proceedings
University of Waterloo, Canada, May 14-17, 2002

AGENT BASED ARCHITECTURES TO IMPROVE SURVIVABILITY OF LARGE COMPLEX CRITICAL INFRASTRUCTURES

Claudio Balducelli, Sandro Bologna

ENEA[1]

Keywords: survivable systems, layered systems, agents architectures, network security

Abstract

Large Complex Critical Infrastructure (LCCI) are worldwide ever more dependent on information systems. The first generation of supervisory and control systems execute their functions inside a monopoly market. The new incoming free market, as well as the need to create more flexibilities and interdependencies between different infrastructures, requires more complex data transmission and control networks, sometimes partially open and interconnected to the public telecommunication networks, such as the Internet. This situation generates new types of risks and vulnerabilities of the whole supervisory and control system. Intruders, hackers and malicious operations could have in the future more and more possibilities to attack LCCI. The roadmaps, under definitions at European Union, aimed to cope with this type of problem are described in the paper. New approaches for modelling LCCIs and analysing their survivability mechanisms are analysed. The electrical power grid control network is illustrated as a special type of LCCI. Considering this type of LCCI, a multi-layers architecture of a society of agents is proposed as a *safeguard layer* aimed to improve the whole electrical grid survivability.

Introduction

During the last years, and especially after the terrorist attack of Sep/11, the importance of protecting complex critical infrastructures has increased and a deeper analysis of their dependability and interdependencies has became a more and more urgent task for all technological and industrial countries.

The term *Large Complex Critical Infrastructure* (LCCI) defines a distributed network of independent, mostly privately-owned, man-made systems and processes working collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services [1].

Electrical power systems network is certainly one of the most important infrastructures of the high industrialised countries. Many other infrastructures are also very critical and interdependent with this one: telecommunication system, natural gas and oil transportation system, water supply system, banking and finance system, auto-route transport system, airways and railways system etc. Generally infrastructures depend on other infrastructure as, for example, the electrical infrastructure depends on oil/gas transportation network to acquire the primary energy sources and telecommunications network for data communication and control [2].

[1] Italian National Agency for New Technologies, Energy and the Environment
Via Anguillarese 301, 00060 Rome (Italy)

Role of European Union in Critical Infrastructures Protection

The economy and security of Europe are increasingly dependent on a spectrum of critical infrastructures, which can be broadly grouped in the following five domains:

- Information and Communications
- Energy (Electrical Power and Oil and Natural Gas Production and Storage)
- Transportation
- Banking and Finance
- Vital Human Services (Emergency Services, Government Services, and Water Supply Systems)

The above five categories of critical infrastructures are highly interdependent, both physically and in their greater reliance on the information infrastructure. This trend has been accelerating in recent years with the explosive growth of information technology and shows no sign of abating. Potential threats to the normal functioning of these infrastructures are both natural and man-made. Individual outages can be serious enough, but this growing degree of interconnectedness can make possible a whole new scale of synergistic, non-linear consequences.

Information societies and, in particular, e-economies are evolving on a trans-national scale. It is thus a genuine task for the EU Commission to support a comprehensive and long-term approach for critical infrastructure protection. As the European economy becomes even more tightly connected through telecommunications, electronic signalling systems, power generation and distribution, information lines, financial networks, transportation systems (road, rail, air, water), and other connections involving critical infrastructures, possible disruptions have far greater potential than ever before to ripple throughout the economy. This unprecedented degree of infrastructure interconnectedness develops into an increasingly enmeshed European economy. In this situation, outage "ripples" in one infrastructure cause cascades of economic malfunction, as individual outages lead to outages in other infrastructures, which in turn intensify the first outages in a firestorm-type of phenomenon. This negative synergy could create havoc in an economy that does not have mechanisms in place to cope with these effects.

At the same time that the information technology revolution has led to substantially more interconnected infrastructures with generally greater centralised control, the advent of "just-in-time" business practices has reduced margins for tolerable error in infrastructures. Any one of these trends would be a cause for uneasiness. The convergence at the same time has no precedent in western economic history. While important steps have been taken on individual infrastructures, the issue of interdependent and cascading effects among infrastructures has received much less attention. This situation calls for concerted efforts of prevention and for building shock absorbers of both a physical and policy nature into our economy in order to protect against major infrastructure breakdown. Yet little is known about what these effects are or how they propagate. Future work on enhancing Critical Infrastructures Protection within the EU will need to be cognisant of all of these problem areas [3].

This finding has been reinforced by the Organisation for Economic & Development (OECD) which warns that: "globalisation, climate change, the transition to a more technology-intensive economy, demographic and societal change, growing interdependencies, to name but a few significant trends, look set to increase the vulnerabilities of major systems during the 21st century. The provision of health services, transport, energy, food and water supplies, information and telecommunications, safety and security are all examples of vital systems which can be severely damaged by a single catastrophic event, a chain of events, or the disastrous interaction of complex systems. There is growing concern that extensive disruption to, or collapse of, these systems could significantly impair future economic and social development"[4].

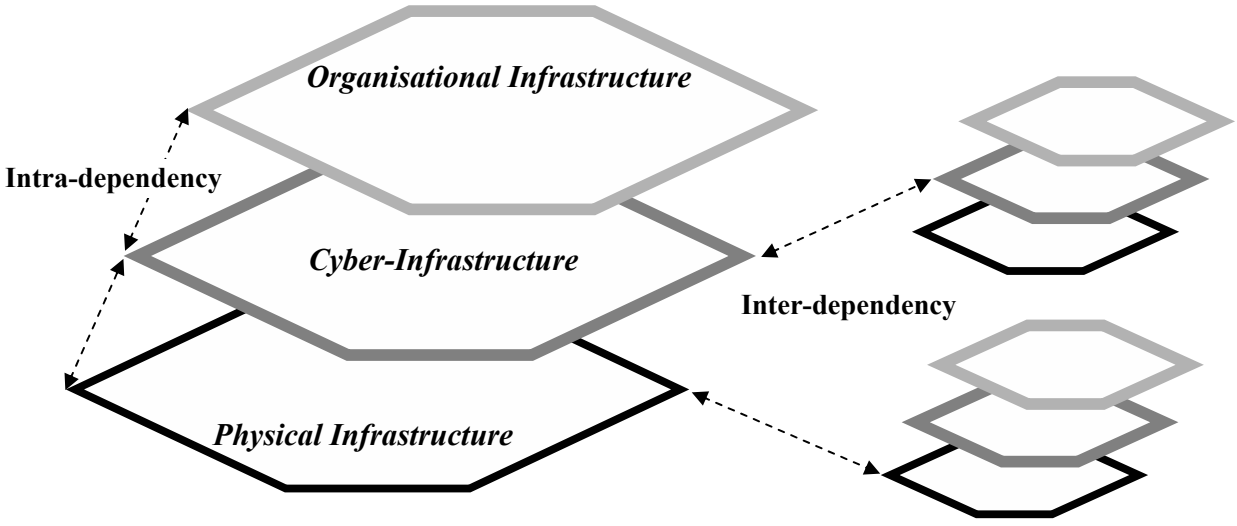
From several years EU has launched a dependability initiative inside the Information Society Technologies (IST) Programme, named the DEPPY initiative (http://deppy.jrc.it). Many recent developments and announcements provide evidence of the great need to define and plan a broader and more fully-integrated set of dependability-related activities, including the growing problem of Critical Infrastructures Protection, for the Framework Programme 6 of the Information Society Technologies (IST FWP6). For such a reason, recently has been issued by the EU a Call for Proposals for strategic roadmaps for applied research, which should provide inputs for the specific subject to IST FWP6.

Layered infrastructures

Software based infrastructures, born from the pervasive computerisation and automation of the physical infrastructures over the last decades, are generally called *cyber-infrastructures*. The Internet data exchanging software protocols establishing network connections between client and server nodes are the most evident examples of the new generation of critical infrastructures. The interdependency between physical and software based infrastructures is called *cyber-interdependency* [5]. The new SCADA-MMS systems are examples of new cyber-infrastructures controlling electric power grids. In this case the vulnerability of the electrical power system doesn't depend only by faults generated inside the electrical network components, but also by attacks against the new types of software systems, sometimes distributed and implemented inside public and not well protected information networks.

Organisational infrastructures are composed by human agents controlling, managing or utilising the functionalities the other types of infrastructures. Organisational infrastructures and cyber-infrastructures have in general a high level of interdependency, some time may be also in competition each other. When a disaster occurs inside a physical infrastructure, is not always clear if the fault was generated by the cyber-infrastructure or by the human operators belonging to the organisational infrastructure.

Figure 1: Inter and Intra dependency of LCCIs



Organisational infrastructure has the lowest degree of formalisation; it changes and is modified along the time, and frequently need to be trained about the correct utilisation of the other infrastructures.

The two types of infrastructures, described above, can be considered interconnected with physical infrastructures to form *layered infrastructures* as shown in fig 1. They are composed by:

- Physical infrastructures (made by hardware components).
- Cyber-infrastructures (made by software components).
- Organisational infrastructures (made by human operators).

As visualised in the figure each infrastructure (physical, software and organisational) could be modelled as a set of components contained in different layers. The layers are dependent on each other by a sort of *intra-dependency*. In the electrical power distribution infrastructures intra-dependency corresponds to the relationships between the physical electrical components and the supervisory/control systems based on EMS/SCADA systems. Intra-dependency realises a *strong dependency* link between infrastructures: generally the first infrastructure could not perform its mission (surviving) if it is not continuously supported by the second one.

The infrastructure physical layer is often connected to the physical layer of other infrastructures. Also in this case we could have dependency (*inter-dependency*) between infrastructures, but in this case it is a *week dependency* link: the first infrastructure could continue to perform its mission alone, at least for a certain time. This is the case, for example, of unavailability in oil/gasoline pipeline network. It could generate consequences on the electrical network only when oil reservoirs of power generation plants will get exhausted.

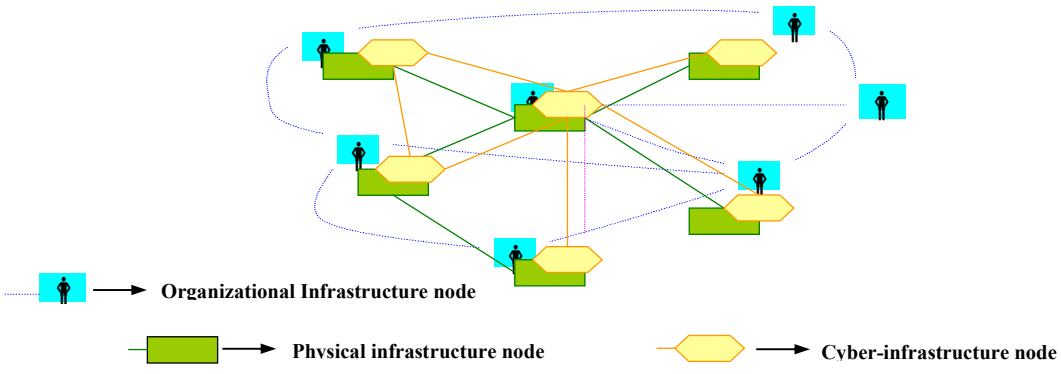
In the last years the cyber-infrastructure layers more and more frequently were interconnected with the cyber layers of other infrastructures. This is due to the increasing of services offered on Internet, new open market opportunities, and the needs of the societies to exchange data and to share software tools.

Infrastructure survivability

Survivability is the ability of a computer-communication system-based application to satisfy and to continue to satisfy certain critical requirements (e.g., specific requirements for security, reliability, real-time responsiveness, and correctness) in the face of adverse conditions [6].

Using multi-layer modelling of infrastructures, it is possible to consider the *multi-layer survivability* concept. In an oversimplified formulation of multi-layer survivability policy, no system or network entity is allowed to depend on an entity that has been assigned a lower survivability level; otherwise faults could easily propagate from less critical toward more critical

Figure 2:Modelling infrastructure as a population of agents



layers. Following the above assumption, in the schema of fig 1, the survivability level of the upper infrastructure layers may be greater that the lower ones, because generally faults and loss of functions could propagate only from upper toward lower layers.

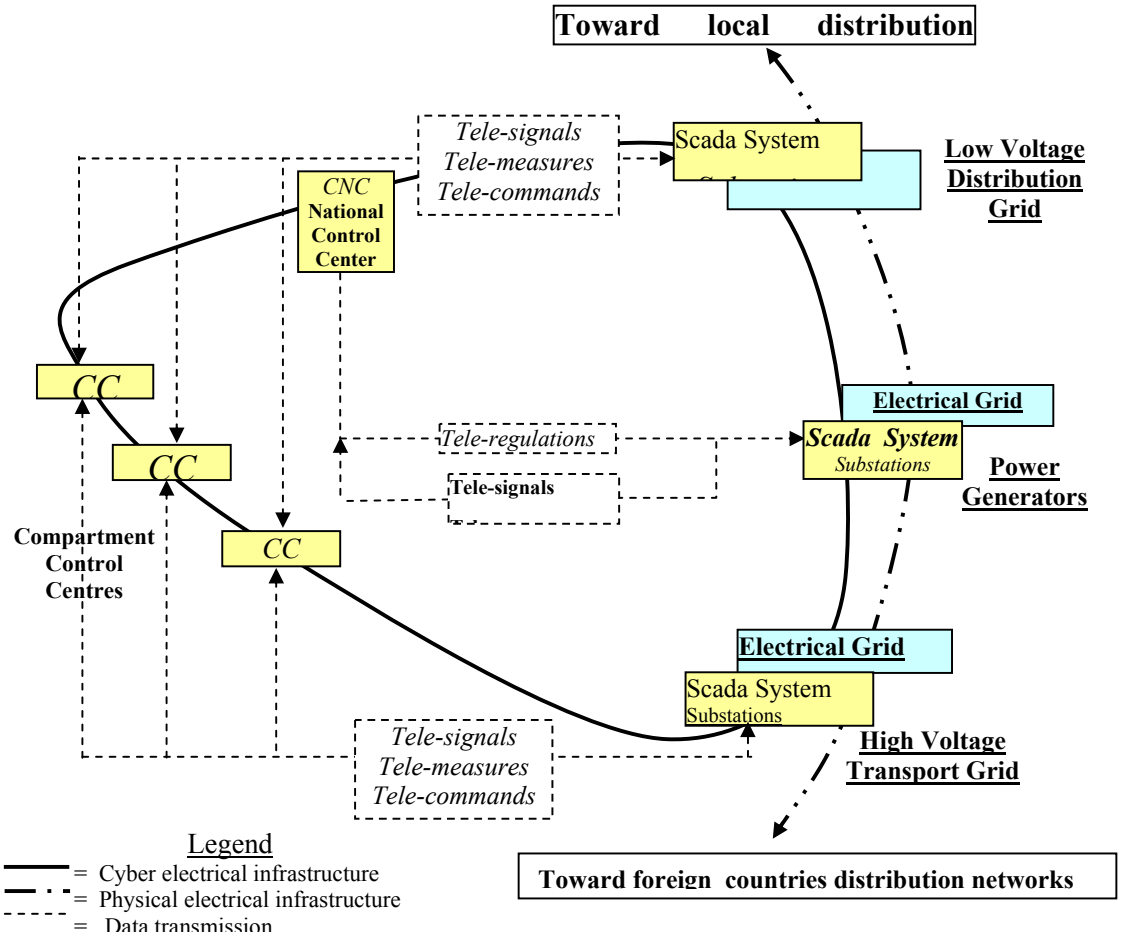
Unfortunately in the last years the survivability of cyber-infrastructures decreased especially for the increasing possibility of electronic attacks following the same patters seen in attacks on Internet e-commerce sites. As interconnections and interdependencies increases, cyber-infrastructures seem to become the most vulnerable part of all traditional infrastructures.

Infrastructures modelling

One effective way to investigate the infrastructure behaviour and criticalities is to view them as an architecture composed by a population of interacting agents. The diagram in fig. 2 shows the concept behind this type of architecture. Here the rectangles represent the components of the physical infrastructure layer, the hexagons the components of the cyber-infrastructure layer (e.g. EMS/SCADA system substations in electricity transmission and distribution domain) and the human figures the organisational infrastructure nodes.

Developing a Safeguard Infrastructure

Figure 3: Layout of electrical network control infrastructure



SAFEGUARD (www.ist-safeguard.org) is an EU project aimed to enhance the dependability and survivability of Large Complex Critical Infrastructures, such as distributed electric and fixed and mobile telecommunication networks.

Regarding the electrical network infrastructure, the introduction of competition in the electric power industry, combined with increased public demand of power, has resulted in greater reliance by power utilities on information systems and networks. Efforts to allow easier access to operational, customer, and supplier information, combined with the expansion of corporate IT boundaries, vastly increases the vulnerabilities of power company networks.

Actually, due to the fact that electrical companies represent a key component of one of the nation's critical infrastructures, these companies are likely targets of coordinated attacks by "cyber-terrorists", as opposed to disorganized "hatchers". Such attackers are highly motivated, well-funded, and may very well have "insider" knowledge.

The main objectives are to develop conceptual and software tools (integrated methodologies, models, methods and middleware) that enhance the dependability, survivability and security of LCCIs, especially focused on the cyber and organisational infrastructures.

Electrical Infrastructure Layout

The National high voltage electrical network supervisory and control system is managed by a National Control Center (CNC) connected with more Regional Control Centers (CC). The control centers exchange data through the telecommunication network with remotely controlled substations working as SCADA/EMS systems (see fig.3).

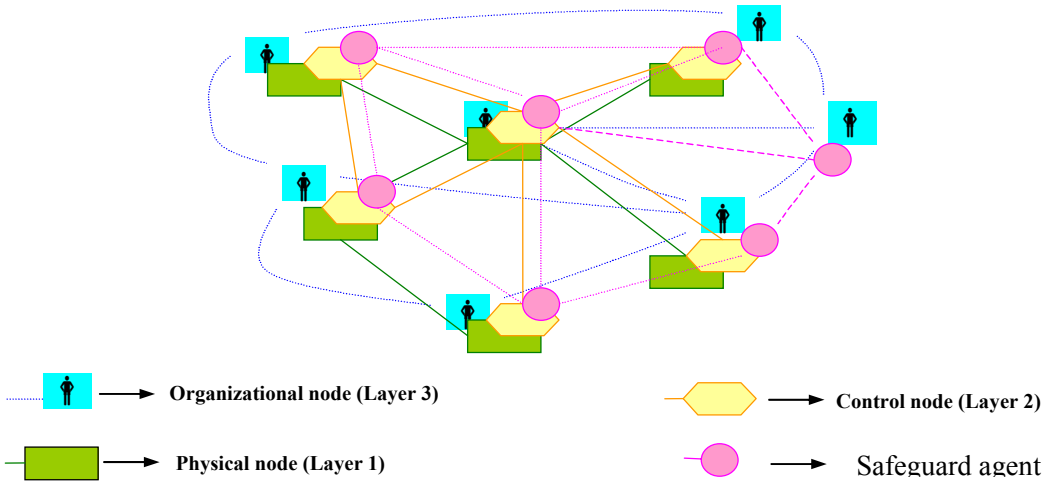
This system represents the middle layer infrastructure of fig. 1, the so-called cyber-infrastructure of the national electricity transport infrastructure. It controls the electrical power company core operations, allows companies to maintain centralized monitoring of their energy management systems (EMS) and transfer power from generation to the end user.

Safeguard agents

As it was shown in fig 2, also the electrical infrastructure could be modeled by as population of agents distributed on three different infrastructure layer:

- Layer 1 represents the physical electrical components of electrical grid;
- Layer 2 represents the control/automation components;
- Layer 3 represent the organizational/supervisory (human) components;

Figure 4: Safeguard agent layer



Electrical infrastructure safeguards could be also modeled, as in fig 4, by a *fourth layer* containing a population of safeguard agents interacting with layer 2 and 3.

The circles represent the SAFEGUARD agents, managing survivability and integrity of the whole infrastructures. One of the aims is to investigate autonomous agents architectures [7] able to manage the survivability of the infrastructure through localised communication, without appeal to a global co-ordinator, or to excessive inter node communication.

The main objective of Safeguard agents is to establish mechanisms able to discover and manage fault conditions arising from layer 2 and/or from the communication protocols working between layer 2 and 3.

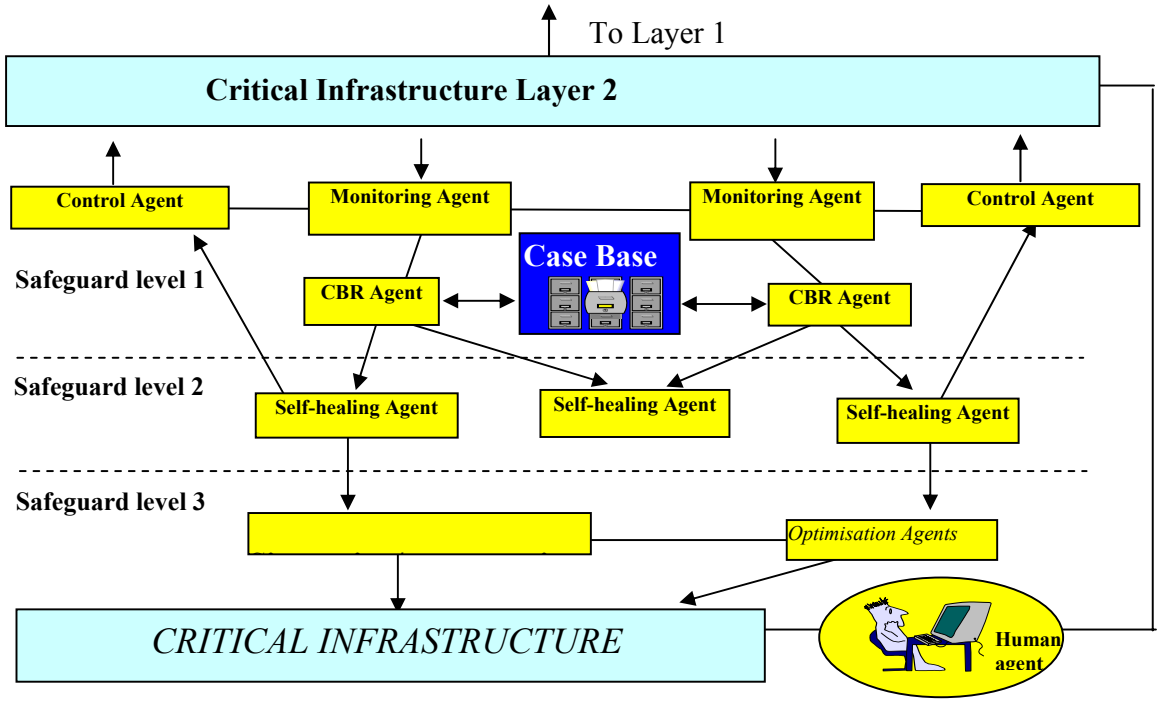
Proposed multi-agents architecture

The Safeguard Agents (SA) are implemented as a society of agents distributed inside three different levels of competences/roles:

- At level 1: predict and indicate if a certain component works in a fault condition or if an attack is in progress;
- At level 2: a self-healing mechanism tries to substitute/repair the functions executed by the fault components;
- At level 3: if self-healing fails, the fault components are isolated and LCCI reconfiguration strategies are suggested.

SA implements a mechanism able to *increment survivability* of layer 2 and 3 components: it will not be sufficient for a simple component malfunction to produce degradation of the whole system. The agents must be able to monitor, substitute, repair or isolate a fault component during a certain time of operations.

Figure 5: SAFEGUARD Multi-agent architecture



To execute functions at level 1 some SA are specialized to monitor (through the network) the behaviour of certain classes of components. Monitoring results are passed to CBR agents (Case Base Reasoning agents) [8], specialised in the fault/attack discovering. They compare the specific component behaviour with a list of *behavioural Cases*: a Case is a collection of indicators of a certain component working condition. They have a memory to store the *normal functioning condition* of the component as Cases inside a Case Base and are able to retrieve a set of faults Cases indicating characteristic statuses in presence of certain faults. The Case Base is initially constructed off-line and periodically updated on-line by some *learning activities* of the agents.

To execute functions at level 2 self-healing agents must actuate the recovery/reconstruction actions inside the infrastructure layer 2. They have the capacity to re-initialise software and procedures inside the damaged layer and substitute/repair the function performed by the fault component.

To execute function at level 3 the agents have some *scheduling/optimisation capacity*. Optimisation algorithms inside dynamic domains could to be adopted [9]. In some case may be sufficient only a *partial and not a complete substitution* of the functions executed by the fault component. In this case the choice of the parts to be substitute could be optimised respect to the objectives that the plant operators could adopt.

Conclusion and future developments

Safeguarding LCCIs seems an important and strategic task for high technological and industrial countries, to avoid unexpected disasters involving the security of the citizens. United States have just experienced some security lacks and vulnerabilities inside their national electrical grid control and supervisory systems. European Union is analysing new roadmaps and methodologies aimed to preventing and managing the principal types of attack scenarios inside the most important LCCIs. SAFEGUARD project is one of the first initiatives in this direction. We hope, in th future, in parallel with the growth and the increasing interconnection of LCCIs, their security and survivability issues will be considered further and taken into account by the public authorities.

References

1. S.M. Rinaldi, J.P. Peerenboom, T.K.Kelly, (2001), 'Critical Infrastructure Interdependencies', IEEE Control System Magazine, Dec 2001.
2. S. Bologna, F. Lambiase, E. Ratto, "Large Scale Electric Power Distribution and Telecommunication Systems Survivability", in Proceedings of ISW-2000, Third Information Survivability Workshop, Oct. 24-26, 2000, Boston, USA.
3. "ACIP – Analysis & Assessment for Critical Infrastructure Protection", proposal submitted under the thematic priorities of the EU Fifth Framework Programme, strategic roadmaps for applied research. Confidential.
4. 'OECD Future projects on Emerging Risks', Available at http://www1.oecd.org/sge/au/risk.htm, Accessed 5 April 2002.
5 Neumann, P.G. (2000) 'Practical Architecture for Survivable Systems and Networks', Available at http://www.csl.sri.com/users/neumann/survivability.html , Accessed 5 April 2002.
6 Sekar R., Cai Y, Segal M., (1998), 'A Specification-Based Approach for Building Survivable Systems', in Proceedings of 21th National Information System Security Conference, Oct 6-9,1998, Crystal City, Virginia
7 Gadomski, A.M., (1997) 'Personoids Organisations: An Approach to Highly Autonomous Software Architectures', in Proceedings of 11th Int. Conf. On Mathematical and Computer Modelling and Scientific Computing, 31/3 – 4/4 1997, Washington D.C.
8 Balducelli, C., Brusoni F. (1996), 'A CBR Tool to Simulate Diagnostic Case Base Operator Models', in Proceedings of European Simulation Symposium , ESS96, Genoa

9 Balducelli, C., D'Esposito, C., (2000), 'Genetic Agents in an EDSS system to optimize resources management and risk object evacuations', Safety Science 35 (2000) 59-73.

Author Biography

Claudio Balducelli is a senior scientist working at ENEA since 1983 in the field of AI technologies applied to operator decision support systems during the emergency industrial events. His interests include operator models, knowledge formalisation, planning, computerised procedures, plant diagnosis, case based reasoning, learning and fuzzy algorithms. Actually he is has in charge the technical management of European Projects in the field of controlling and safeguarding Large Complex Critical Infrastructure.

Sandro Bologna is graduated in Physics at University of Rome. He has about 30 years experience at ENEA, where he has covered different positions as Researcher, Head of Research Units, Head of Research Projects at national and international levels. His main research activities deal with the achievement and assessment of system safety and reliability, operator decision support systems for plants and emergency management, plant control room design and assessment. In this field he has co-authored several publications and books.