NETWORK SECURITY
in critical infrastructures
NETWORK SECURITY
in critical infrastructures

Authors:

Stefano AMICI (Enav S.p.A.),
Riccardo BIANCONI (SINCERT),
Danilo BRUSCHI (Milan University),
Bruno CARBONE (Enav S.p.A),
Giancarlo CAROTI (Terna S.p.A. – National Power Grid)
Valentino DI TOMA (Ancitel S.p.A.),
Silvio FANTIN (GRTN S.p.A),
Giovanni FASSINA (Poste Italiane S.p.A.)
Luisa FRANCHINA (Superior Institute for ICT),
Vincenzo GESMUNDO (Selenia Communications S.p.A.),
Carlo GUGLIELMINI (Selenia Communications S.p.A.),
Maurizio MAYER (AICT),
Giulio MICELI (AICT),
Massimo PANICHELLI (Ancitel S.p.A.),
Giovanni PATELLA (Communication Ministry),
Daniele PERUCCHINI (Ugo Bordoni Foundation),
Armando PERUGINI (Captain (Ret) Italian Navy - Defense Ministry Consultant
TELEDIFE-SE.PRO TE.C. S.A.S),
Rodolfo PERUGINO (Poste Italiane S.p.A. – Italian Postal Service),
Gian Luca PETRILLO (Communication Minister Advisor),
Massimo PICCIRILLI (Communication Ministry),
Francesco PIRRO (CNIPA),
Gian Luigi PUGNI (Enel Ape s.r.l),
Giovanna RICCI (Rete Ferroviaria Italiana S.p.A. – Italian Railways),
Giovanna SAMOGGIA (Rete Ferroviaria Italiana S.p.A.– Italian Railways),
Federico SANDRUCCI (Commodore (Res.) Defense Ministry Consultant T
ELEDIFE-SE.PRO TE.C. S.A.S ),
Alberto SARTI (Finmeccanica S.p.A.),
Gianluigi SCAZZOLA (Selenia Communications S.p.A.),
Stefano SCIASCIA (Information and Security Department
– Italian Defense Ministry),
Roberto SETOLA (Prime Minister’s Office – Department for Innovation,
Technology and University Education – Rome Biomedical
Research Center),
Gigi TAGLIAPIETRA (Siosistemi S.p.A),
Guido TRIPALDI (I.NET S.p.A.),
The opinions and remarks expressed in this book, as well as suggested proposals, only reflect the views of single participants and not of the Institute and Companies they belong to. The contents of this book should only be considered as a general reference technical/scientific study on network-security and communication-protection related issues. Therefore, both the writers and the Superior Institute for ICT, editor of this book, shall not be held liable for any consequence deriving from any possible use of its contents.

References made to specific brands or product names should only be meant as examples and do not provide and exhaustive description of all the products found on the market. Such references should not be considered in any way as an assessment or indication related to the use of specific products.

This book is available for free and the writers have granted the Superior Institute for ICT free use of their writings, indefinitely waiving their right to any copyright-related claim.
Index

Introduction 7

Reader’s Guide 15

1. General Remarks 17
   1.1 Introduction 17
   1.2 CNI and CII: Interdependence and Protection 19
   1.3 Aims of This Book and Working Group Activities 25
   1.4 Current International Initiatives for CII Protection 27
   1.5 The Italian Situation 36
      1.5.1 Specific Activities for Network Security

2. Critical National Information Infrastructure Protection 39
   2.1 Introduction 39
   2.2 Critical National Information Infrastructure Protection 39
      2.2.1 Technology Evolution and ICT Infrastructure Dependence
      2.2.2 Security Issues in Critical Information Infrastructures
         2.2.2.1 General Remarks
         2.2.2.2 Specific Critical Issues associated to Critical Information Infrastructures
            2.2.2.3 Interdependencies between Critical Information Infrastructures
               2.2.2.3.1 Operative Interdependencies
               2.2.2.3.2 Logical Interdependencies
2.2.2.3.3 Geographical Interdependencies
2.2.2.4 Threats
2.2.2.4.1 Definition
2.2.2.4.2 Classification
2.2.3 Security Management
2.2.3.1 Context Identification and Modeling
2.2.3.2 Threat, Impact and Vulnerability Analysis
2.2.3.2.1 Threats against CII and Related Communication Systems
2.2.3.2.2 Specific Vulnerabilities of CII Communication Systems
2.2.3.2.3 Threat-Service Correlations
2.2.3.3 Risk Assessment and Analysis
2.2.3.4 Risk Management Strategy Definition
2.2.3.5 Choice Effectiveness Verification
2.2.3.6 Operation Procedure Simulation and Testing
2.2.3.6.1 Operation Procedure Testing
2.2.3.6.2 Accident Simulation
2.2.4 From CII Protection to Related Communication Systems

3. Communication Network Protection 69
3.1 Introduction 69
3.2 Communication Networks for CII Structures 69
3.2.1 Functional performance for sensitive communication networks for service guarantee purposes
3.2.2 Solutions for communication networks
3.2.2.1 Current networks for CII infrastructures
3.2.2.2 Networks (and their interaction) model to achieve the requested performances
3.2.2.2.1 Preamble
3.2.2.2.2 Basic network security requirements
3.2.2.2.3 Characterization of network types
3.2.2.2.4 Periodic maintenance of production system
3.2.2.2.4.1 Security auditing and certification
3.2.2.2.4.1.1 The Common Criteria
3.2.2.2.4.1.2 ISO/IEC IS 17799-1 and BS7799-2 89 standards
3.2.2.4.2 Security certification in Italy according to the Common Criteria (and ITSEC)

3.2.2.4.2.1 Accreditation for voluntary certification according to the BS 7799-2:2002 standard

3.2.2.5 Network architectures supporting Critical infrastructure

3.2.2.5.1 Secure network types

3.2.2.5.1.1 Maximum security networks

3.2.2.5.1.2 Secure networks

3.2.2.5.1.3 Robust networks

3.2.2.5.2 Network types - Connectivity

3.2.2.5.3 Network federation

3.2.2.5.3.1 Preamble

3.2.2.5.3.2 Federation agent

3.2.2.5.4 Network access - Network port

3.2.2.5.5 Security Structure at the Middleware - Application - Procedure level

3.2.3 Network power supply systems

3.2.3.1 Standby systems

3.2.4 Data Centre Security issues

3.2.4.1 Environment and borders

3.2.4.2 Building structure

3.2.4.3 Technological plants

3.2.4.3.1 Local Loop

3.2.4.3.2 Electrical system

3.2.4.3.3 Air conditioning system

3.2.4.3.4 Fire system

3.2.4.3.5 Access control

3.2.4.3.6 Monitoring and alarm systems

3.2.4.4 Emergency procedure training for the staff

3.2.5 Emergency networks

3.3 Management and organizational issues

3.3.1 Joint management of crisis situations caused by ICT infrastructures

3.3.1.1 Crisis Unit
3.3.1.2 Identification of the people in charge of CII and ICT emergency management
3.3.1.3 Interaction, integration and interoperability modes
3.3.1.4 Joint training activity and support tools
3.3.1.5 Good rules for ITC emergencies management, including Call Centre
3.3.1.6 When and how to perform ICT emergency simulations
3.3.1.7 Communication issues of Joint Crisis Management
3.3.2 National and world trends
3.3.2.1 Technological and Organizational trends
3.3.2.1.1 Intelligent SW Agents
3.3.2.1.2 IPv6 protocol
3.3.2.1.3 Smart Communication Nodes
3.3.3 The Human Factor
3.3.3.1 Promotion of awareness raising program
3.3.3.2 Actions taken by other countries
3.3.3.3 Personal and procedural countermeasures expected by the Italian National Security Authority (Autorità Nazionale per la Sicurezza - ANS)
3.3.4 Recommended Contractual Framework
3.3.4.1 Additional suggestions

4. Conclusions

Appendix 1 Acronyms and abbreviations
Appendix 2 Reference documents
Appendix 3 Reference standards and regulations
Appendix 4 A risk management application: the TERNA case
Appendix 5 Self assessment questionnaire on the minimum network security requirements
Index of Figures

Figure 1  Interdependence between different CNI/CII Sectors  18
Figure 2  Multi-layer infrastructural model, developed by ENEA for the Safeguard European Project  23
Figure 3  Scope of CIP and CIIP definitions [CiSP]  24
Figure 4  Malfunction Tolerability  41
Figure 5  Risk Analysis Stages  62
Figure 6  Fundamental network security services (ISO)  74
Figure 7  Specifications and test in relation to the assessment level  87
Figure 8  PDCA model applied to ISMS processes  91
Figure 9  CC-based assessment and certification process scheme  96
Figure 10  BS7799-2-based certification scheme  98
Figure 11  Typical components of a Maximum Security Network  100
Figure 12  Example of network connectivity  108
Figure 13  Network federation  110
Figure 14  Network Port  114
Figure 15  Example of PKI Architecture  119
Figure 16  PKI operating mode  120
Figure 17  PKI Architecture  123
Figure 18  Distributed RTC Architecture  125
Figure 19  Joint Crisis Management Unit  135
Figure 20  Possible operational flow  137
Figure 21  «Ad-hoc» national network  145
Figure 22 One application of the RETSINA architecture
Figure A4.1 Terna’s CNI
Figure A4.2 NTG operation and monitoring process components
Figure A4.3 Functional blocks representation of the CII
Figure A4.4 Parts subject to potential threats/vulnerabilities
Figure A4.5 Cause-effect diagram (Ishikawa)
Figure A4.6 Example of a probability/impact curve

Index of Tables

Table 1 A comparison between the OECD document and the UN Resolution 34
Table 2 Example of Correlation Table between Operations and Critical Services 42
Table 3 Threat Partition 54
Table 4 Example of Threats against Communication Links 57
Table 5 Services/Threats 58
Table 6 CNI network requirements 70
Table 7 Examples of CII networks in the Italian scenario 77
Table 8 Architectural Characteristics of CII Networks 78
Table 9 Main characteristics of a Maximum Security Network 101
Table 9 Main characteristics of a Maximum Security Network (Cont.) 102
Table 10 Main characteristics of a Secure Network 104
Table 10 Main characteristics of a Secure Network (Cont.) 105
Table 11 Main characteristics of a Robust Network 106
Table 11 Main characteristics of a Robust Network (Cont.) 107
Table 12 Actions and Recommendations included in the document [5] 152
The idea for this book came from an initiative involving the Istituto Superiore delle Comunicazioni e delle Telecomunicazioni, the Observatory for Communication Network Protection and Security, together with a number of authors from various public and private entities.

The Istituto Superiore delle Comunicazioni e delle Tecnologie dell’Informazione (Institute in the document’s remaining) was established in 1907 as a technical-scientific department belonging to the Communication Ministry. Its main activity is specifically addressed to ICT Companies, government agencies and users and is essentially focused on legislation, experimental activities, fundamental and applied research, specialized training and education in the TLC field.

One of the Institute’s main missions is its proactive role in national and international law-making activities, in order to ensure greater transparency and better access to services for users, manufacturers and TLC network administrators alike.

In this specific context, the Institute plays a two-fold role: through CONCIT (a Coordination Committee recognized at European level which also includes CEI - Italian Electrotechnical
Committee and UNI-National Italian Unification Agency) it transposes European legislation into national law and, at the same time, acts on behalf of the Administration by providing guidance and support to national groups sitting in various commissions and technical research groups belonging to the ITU (International Communication Union), CEPT (Conference European des Postes et Telecommunication) and ETSI (European Telecommunication Standard Institute).

The Institute runs the Post-Graduate Specialization School in TLC (which began its activity in 1923), which provides higher education in electronic communication and information technologies, and issues a specific degree. Following an agreement signed with the Engineering Department of the “La Sapienza” University of Rome, the School organizes yearly courses which also include laboratory activities, workshops and internships.

The Institute also provides technical training and updating courses on electronic communications and information technologies, security, multimedia applications, and Quality of Service to both Ministry and government staff in general, to enhance their technical know-how and skills.

For this reason, the Institute has established a Test Center accredited with the AICA, to issue the European Computer Driving Licence - ECDL.

Furthermore, the Training Center on ICT Security for Public Administration personnel is in the process of being established. The Training Center will provide training and raise awareness amongst government employees on ICT security, through the development of a centralized and coordinated Training and Awareness-Raising Plan aimed at disseminating security principles and methodologies throughout the Administration.
The Institute also promotes educational activities for the general audience through specific events and provides information about its activities and research projects.

As far as research is concerned, the Institute is essentially focused on developing and improving TLC and IT related services. Hence, activities involve almost all areas in these fields, from telephony to television, to signal processing and treatment, from network architecture to service implementation.

Thanks to the manifold skills and resources it can rely on, the Institute takes active part in several European projects for technology development and makes ample use of European funds. Such activities are carried out either independently or jointly with other Research Institutions, Universities and International Study Centers.

As for Information Society activities, reference should be made to a number of projects, some of which carried out together with the Ugo Bordoni Foundation (FUB) in the field of teleworking, IT security, remote learning and access to communication services for disabled or elderly people.

Thanks to the Institute’s support, over the last few years the Ministry was able to implement a number of initiatives to introduce new technologies and systems in communication networks. For example, several feasibility studies were carried out on the application of new TV and multimedia technologies and services, a feasibility study on the provision of macroregional digital satellite TV services and a study for the development of a European satellite system to provide multimedia and interactive broadband services. Another initiative worth mentioning is the Institute’s participation in the EU IST (Information Society Technologies) research and technology development project called ATLAS.

Considering its role as a nonpartisan public institution, the
Institute’s value added in terms of reliability and expertise is the aspect which characterizes the technical support and consultancy services it provides to businesses and entities in the TLC sector.

In addition to traditional certification activities, which are carried out thanks to the Institute’s skills and laboratory equipment - which allow for any telematic device to be tested against existing legislation or reference recommendation - other activities involve specific measurement campaigns to monitor quality of service (QoS), network security and to verify specific service interoperability techniques for network interconnection purposes.

The Institute manages the number attribution database for the national telecommunication network and number portability for GSM and UMTS devices. It also manages the National Reference Clock (NRC) to synchronize the Italian Numerical Telecommunication Network and provides institutional support to those who take part in the calls for proposals for the E-TEN (Trans European Network for TLC) EU program. The Institute works with several Certification Bodies to verify and control Corporate Quality System compliance with UNI EN ISO 9000 standards, is involved in monitoring Accredited Laboratory compliance with UNI CEI EN ISO/IEC 17025 rules and is a Notified Body for activities envisaged by Legislative Decree n. 269 of May 9, 2001. The Institute acts as a Certification Body for commercial security systems and products (OCSI), and is an Evaluation Center (Ce.Va.) for ICT systems and products dealing with classified data. It is also a Notified Body under the EU Directive on radio equipment and telecommunications terminal equipment as well as a Competent Body and Notified Body on electromagnetic compatibility. In 2002, the Institute became the International Certification Body for the TETRA MoU.

This book was published also thanks to the contribution provided by experts from the Observatory for Network Security and Communication Protection.
The Observatory for Network Security and Communication Protection is chaired by the Communication Ministry Secretary General and it includes representatives from the Ministries of Communications, Justice, Internal Affairs, Defense, Industry and the Departments for Civil Service and Innovation and Technology of the Prime Minister’s Office, who are appointed through ad-hoc ministerial decrees jointly issued by the Ministers of Communication, Justice and Internal Affairs.

Amongst the observatory’s tasks, we shall mention the following:

a) monitoring the industry’s technology development, with a specific focus on security;

b) providing assistance and advice on technology-related issues to those government agencies who express the need to make their “sensitive areas” more secure;

c) defining a required “minimum security level” to have access to public networks;

d) making suggestions for the protection of civil infrastructures against electronic and electromagnetic attacks;

e) giving indications on security standard certification and development for TLC services and facilities;

f) promoting awareness-raising through specific information campaigns.
This book is part of a number of activities carried out by the Communication Ministry in 2004, with the aim of introducing guidelines on the following topics:

- NETWORK SECURITY – FROM RISK ANALYSIS TO PROTECTION STRATEGIES
- NETWORK SECURITY IN CRITICAL INFRASTRUCTURES
- QUALITY OF SERVICE IN ICT NETWORKS

We would like to seize the occasion to thank all those who, with their enthusiasm and professionalism, have contributed to the drafting of this document:


Selenia S.p.A.), Maurizio MAYER (AICT), Giulio MICELI (AICT), Massimo PANICHELLI (Ancitel S.p.A.), Giovanni PATELLA (Communication Ministry), Daniele PERUCCHINI (Ugo Bordoni Foundation), Armando PERUGINI (Capt. Italian Navy (Ret) Defense Ministry Consultant-TELEDIFE-SE.PRO TE.C. S.A.S), Rodolfo PERUGINO (Poste Italiane S.p.A. – Italian Postal Service), Gian Luca PETRILLO (Advisor to the Communication Minister), Massimo PICCIRILLI (Communication Ministry), Francesco PIRRO (CNIPA), Gian Luigi PUGNI (Enel Ape s.r.l), Giovanna RICCI (Rete Ferroviaria Italiana S.p.A., Italian Railways), Giovanna
Introduction


We also thank the following people for their contributions and suggestions:

Pierpaolo ARGIOLAS (Rete Ferroviaria Italiana S.p.A., Italian Railways), Diego BISCI (Terna S.p.A. - Rete Elettrica Nazionale, National Power Grid), Maurizio BONANNI (Communication Ministry), Davide BRACCINI (ABI Lab Consortium), Giuseppe CAPORELLO (Internal Revenue Service – Central Auditing and Security Directorate), Marco CARBONELLI («Ugo Bordoni» Foundation), Mario CICLOSI (Interior Ministry), Mario Carlo DI GIORGIO (Finance Ministry), Antonio GRUPPINO (Rete Ferroviaria Italiana S.p.A., Italian Railways), Salvatore LEOTTA (Electronic Data Systems Italia S.p.A.), Alessandro LORENZINI (CommScope Solutions Italy S.r.l.), Stefano LUBERTI (Enel Holding S.p.A.), Mariano LUPO (Finance Ministry-DFP/UTI V Dept.V – Technical Regulations), Renato MAREGA (Nergal S.r.l.), Antonio MENGHINI (Electronic Data Systems Italia S.p.A.), Stefano Aurelio MOLINARI (Selenia Communications S.p.A.), Claudio PETRICCA (Higher Institute for ICT), Gianfranco PONTI VOLEPE (CNIPA), Luciano PUCCI (Interior Ministry), Michele RINALDI (Finance Ministry – Tax Policy Department), Mauro SARTI (Anixter S.r.l.), Romano STASI (ABI Lab Consortium),
Maurizio TALAMO («Tor Vergata» University - Rome), Mario TERRANOVA (CNIPA), Paola TOGNETTI (Finance Ministry – Tax Policy Department), Salvatore TURANO (Ancitel S.p.A.), Raffaele VISCIANO (Finance Ministry-Tax Policy Department).

Rome, March 2005

*Luisa Franchina, PhD*

General Director
of Istituto Superiore delle Comunicazioni
e delle Tecnologie dell'Informazione.
This document summarizes work carried out by the “Critical Infrastructure” group in which representatives from several public institutions, critical Italian infrastructures and Companies working on TLC network security took part.

This working group was established because of the need to analyze possible implications for critical infrastructure security and operational continuity coming from new socio-economic and technical challenges, also considering the essential role TLC infrastructures now play with respect to all critical national infrastructures. This situation has led to greater interdependence between different infrastructures, mostly due to the huge spread of ICT. Furthermore, it has to be considered the huge increase in the number of threats affecting infrastructures, deriving from both natural disasters and criminal acts, especially terrorist attacks.

As pointed out in Chapter 1, these reasons led to the introduction of several national and European initiatives aimed at enhancing the overall security of critical infrastructures, which are defined as Critical Infrastructure Protection strategies.

The following chapter will describe the new architectural scenario characterizing national infrastructures, focusing on those elements of interdependence and related threats that must be considered to properly manage infrastructure security and operational continuity.

Chapter 3 delves into Best Practices or Good Rules in communication network protection, not only due to their importance as
such, but also because their working properly is essential to make sure that other critical infrastructure might do their work.

For this reason we shall analyze the specific aspects which characterize the communication networks which support critical national infrastructures, highlighting each component’s importance. A specific section is dedicated to security certification and its importance in increasing user confidence concerning viable security levels.

For these infrastructures, security cannot just be limited to mere technological aspects (despite their remarkable importance), but it should also provide for an appropriate organization which is capable of managing crises effectively, as well as appropriate training for all employees who are involved in some way or another in infrastructure management and use.

Several R & D activities are currently in place to identify technology solutions which might be better suited to the changed infrastructural context.

Chapter four reports on the main conclusions we might draw from this work.

This book also includes a number of appendices: one is dedicated to various reference and legislative standards; another one provides a detailed description of guidelines on which the business continuity plan prepared by an important critical infrastructure operator is based and, lastly, a self-assessment questionnaire is provided, which might be useful as an initial TLC infrastructure security analysis tool for people who have the responsibility of managing critical infrastructures.
1 – General Remarks

1.1 INTRODUCTION

The development and organization of industrialized countries are based on increasingly complex infrastructure systems: the so-called Critical National Infrastructures (CNI). They are defined as any public or private infrastructure whose operation is essential for a country’s security and functioning.

Such infrastructures oversee fundamental sectors for modern societies such as health care, the economy, energy, transport and communication systems, law enforcement, defense and, in general, public administration.

They can be affected by critical events of different nature, which are able to jeopardize their efficiency both directly and indirectly. Generally speaking, critical events are usually related to intentional attacks or natural disasters.

In order to work, CNIs increasingly rely on TLC infrastructures. (CII - Critical Information Infrastructures). These networks must guarantee CNIs’ operational viability under normal working conditions, but especially and more importantly when critical events occur.

However, critical events might not only involve CNIs, but also their related TLC infrastructures.

Furthermore, both CNIs and CIIIs might be subject to failures which are not caused by external events.
In this context, we shall refer to Critical Information Infrastructures (CII) as those Critical National Infrastructures which totally or partially rely on one or more information infrastructures\(^1\) for their monitoring, control and management.

Such information infrastructures must allow CNIs to operate under normal working conditions and they should also guarantee a commensurate operative capability in case of an emergency, that is when critical events occur.

We should not even underestimate the high degree of interdependence existing between several Critical Infrastructures. As a matter of fact, at a very high level, it is possible to provide a hierarchical description of the interdependence existing between different sectors as follows (Fig. 1):

\[\text{Figure 1: Interdependence between different CNI/CII sectors}\]

\(^1\) In literature, the CII acronym also refers to “Critical Information Infrastructures”, giving greater importance to protection aspects specific to the cyberspace and in particular Internet.
As it might be observed, the highest ranking factor is Country: the regular development of a Nation’s economic and social life strongly depends upon the quality of a number of underlying essential services.

In a nutshell, the most important pillars are Energy and TLC (and related IT), as well as “value-added” services such as Health Care, Civil Defense, and so forth, which anyhow rely on the first two pillars.

By definition, Energy is the element without which no job can be done. Therefore, any advanced service depends upon a proper energy production, transmission and distribution.

TLC and IT are the elements without which no signal, data or information transmission is possible and hence, the appropriate coordination of both local and remote (human and technological) resources is not possible either.

However, Energy and Telecommunications are mutually interdependent: without adequate and steady power supply, ICT equipment cannot work and power production, transmission and distribution grids can work only if communication systems are able to connect different facilities.

More specifically, the aim of this document is to provide a number of initial proposals concerning critical issues related to the interdependence existing between traditional CNIs and TLC infrastructures, including also Information and TLC networks proper.

Document aim is to provide CNIs with basic indications on how to adequately set up their communication systems, in order to guarantee the necessary effectiveness also in emergency situations.

1.2 CNI AND CII: INTERDEPENDENCE AND PROTECTION

CNIs, despite the specificities deriving from their respective tasks, share a number of common features:

- They are all widely distributed throughout the national territory
- High visibility
- Difficulties in keeping all facilities under surveillance
- Potential coordination and intercommunication problems

• They all have a public service mission
  - Severe availability and reliability requirements
  - Rapid reaction and recovery characteristics in times of crisis
  - Infrastructures characterized by maximum resilience and security
  - Potential repercussions on public safety

• They must provide for interoperability with external public and private users/clients.
  - High intrusion risk
  - They require controlled and secure access points for multi-protocol communications
  - Important economic consequences due to failures/sabotage.

Critical national infrastructures include the following:

• Energy transmission and distribution networks (electricity, gas, etc.)
• TLC networks
• Transport systems (goods and passengers)
• Emergency services
• Defense infrastructures
• Banking and financial circuits
• National health care services
• Water transport, distribution and treatment systems
• Media and public information networks
• Farming and food processing industries
• Government networks
Several events might totally or partially affect infrastructure efficiency in one or more Countries: natural events (floods, earthquakes, volcanic eruptions), events caused by voluntary (terrorism, cyber-crime) or involuntary (errors, omissions) human actions, events affecting the environment (pollution, chemical substances, fires), events related to equipment malfunctions (hardware failures, software bugs, etc.).

The recent report published by the Canadian government on the security of its CNIs [8] shows that over the next few years the scenario will be characterized by a remarkable increase in the number of threats related to natural events (due to extreme climate changes) and criminal actions (linked to the current social and political context, especially terrorism).

This last aspect is related to a number of independent causes which, unfortunately, are also concurrent. On the one hand, the spread and importance of IT at all levels of CNI management and control is such that they have become privileged targets for both traditional criminal activities and cyber-crime. Hence, CNIs must take into account, in addition to “traditional” physical threats, also those threats which might directly or indirectly exploit information technology.

By the same token, increased terrorist threats must be considered also, which might target CNIs to wreak havoc in several countries and cause uncertainty amongst their citizens. Terrorist activities which might only be limited to providing “support” to other kinds of criminal actions in order to enhance their effect and/or delay rescue and recovery operations, thereby magnifying their media impact.

As was already underlined in the document entitled “CII Protection – The Italian Situation”\(^2\), in addition to threats we also have to remember that the CNIs’ architectural scenario is changing rapidly and profoundly.

\(^2\) Written in March 2004 by the working group established by the Department for Innovation and Technology of the Prime Minister’s Office
As a matter of fact, “up to ten years ago, each of these infrastructures could be considered as a substantially independent and self-sufficient system, managed by vertically integrated operators. For a number of reasons, the structure has gone through a profound change so that now all infrastructures tend to be interdependent, especially since they now share the so-called cyberspace, i.e. the virtual space produced by the interconnection of computers, telecommunication systems, application and data. Therefore, any (accidental or willfully caused) failure in any infrastructure can easily extend to other infrastructures, according to a domino effect, magnifying its effects and causing malfunctions and dysfunctions also to users who are quite remote, both geographically and functionally, from the place where the initial failure occurred”. [1]

The power failure which affected most of the US North-East coast in August 2003 is a remarkable example of how a simple malfunction in a few modules of a distribution company’s IT control system, joined with a number of other accidental events, might lead to the almost complete paralysis of all local infrastructures causing billions of dollars in damage.

This is also due to the fact that, following the widespread use of Information Society technologies, Critical Infrastructures have developed a growing interdependence whereby events happening in one specific sector might have an immediate impact on all others. In particular, natural events or criminal actions affecting one CNI, lead to a multiplication and magnification of effects so that even minor events might cause serious and widespread damage.

Therefore, the current scenario is characterized by both greater and more diversified threats against CNIs, as well as by a different infrastructural context which, because of existing interdependencies, engenders a new kind of vulnerability. This requires a greater and different attention towards all aspects related to each individual CNI’s protection, security and robustness, in order to protect national CNIs.

This infrastructural scenario is also going through deep change: infrastructures are now expected to provide innovative and extremely high quality services while, at the same time, preserving their efficiency and cost-effectiveness. This requires the best possible use of each country’s technology infrastructures which can only be achieved
through the massive introduction of advanced automatic control systems and, more in general, through the use of ICT.

In order to better understand the crucial role played by all aspects related to ICT security for critical infrastructure protection, it is useful to refer to the diagram in Fig. 2. Every CNI can be described as a complex structure built over physical, cyber, organizational and strategic layers. Within each CNI, functional links exist between different layers and, at the same time, dependence and interdependence relations exist between the corresponding layers belonging to different CNIs.

Figure 2: Multi-layer infrastructural model, developed by ENEA for the Safeguard European project.
The widespread use of ICT has led to an ever increasing importance of both the cyber-layer within each infrastructure and of the interdependencies existing between the same layers in different infrastructures.

We must point out that, in this context, the term cyber-layer does not correspond to corporate information systems but, rather, to that part within these systems which is entrusted with managing and controlling the infrastructure’s physical layer.

In this framework, as can be seen in Fig. 3, within the broader issue of Critical Infrastructure Protection – CIP, the protection of such “Control and Supervision” layer is what is commonly indicated as Critical Information Infrastructure Protection – CIIP.

Within Critical Infrastructure Protection strategies, CIIP has become a central and increasingly important element.

The term CIIP (Critical Information Infrastructure Protection) refers to all those actions that are meant to enhance security, reliability and appropriate operation for all those critical infrastructures which totally or partially use any information infrastructure for monitoring, management or control purposes.

Figure 3: Scope of CIP and CIIP definitions [CiSP]
Therefore, if we go back to the definition laid down in [1], we can say that CIIP includes all those actions that are meant to enhance security, reliability and availability for all those critical infrastructures which totally or partially use any information infrastructure for monitoring, management or control purposes.

Such initiatives are not limited to the IT security of the cyber-layer, but include all aspects related to service continuity and regularity.

1.3 AIMS OF THIS BOOK AND WORKING GROUP ACTIVITIES

This Report summarizes work carried out in March 2004 by the Working Group which was established within the Communication Ministry.

The Working Group, made up by representatives of the most important public administrations, together with representatives coming from some of the main Italian CNI operators and specialized Companies in this field, focused on the role played by TLC infrastructures with respect to CNI security and service continuity.

The Working Group, benefiting from each member’s expertise, has tried to bring together needs and possible solutions, in order to provide CNI managers with guidelines, or best practices, which might lead to greater effectiveness and awareness in the use of necessary and existing communication systems.

The Working Group analyzed the following aspects:

• Quality of Service and TLC Network Security, also considering International and National Reference Standards and Legislation;

• problems caused by interdependence between CNIs and between CNIs and TLC infrastructures;

• identifying main threats against TLC infrastructures used by CNIs;
• identifying a minimum set of security parameters in order to qualify the security status of TLC infrastructures supporting CNIs;

• identifying minimum technical parameters to guarantee adequate Quality of Service (QoS) providing for the least possible critical situations;

• identifying a number of technical parameters, transparency elements and legal terms which should be used in commercial contract relations and in Service Level Agreements (SLAs) signed with TLC service Providers;

• potential roles Institutions might play to identify and implement common protection strategies;

• Some proposals to self-assess current vulnerability and organization statuses within each CNI.

The following aspects were not considered:

• problems referring to critical components that are not IT-based, are not involved in TLC activities, are peculiar to each CNI (e.g. water or gas distribution systems) and might lead to total failure in case of failure or attack;

• Security issues related to Platforms and Management Applications used by Companies who own CNIs, but that are not directly linked to critical component management (e.g. ERP, payroll systems, database, etc.).
1.4 CURRENT INTERNATIONAL INITIATIVES FOR CII PROTECTION

The first studies on security and service continuity problems for critical information infrastructures were started in the 1990s.

The US was the first country to think about specific government actions on this issue which, in 1998, resulted in the issuance of Presidential Decision Directives 62 and 63.

Since then, several other industrialized countries have developed actions aimed at:

- understanding critical and vulnerable elements of each country’s critical infrastructures, highlighting their weaknesses;
- laying down strategies to mitigate such weaknesses;
- raising awareness amongst service providers on the issue of critical infrastructure protection;
- developing emergency and recovery plans to be implemented in case of negative events affecting one or more critical infrastructures;
- supporting the development of inherently secure technologies;
- Supporting international cooperation.

The issue of Critical Information Infrastructure protection, due to its transnational scope, was recently submitted to the attention of several international institutions.

In March 2003, the first meeting of G8 country experts on CIIP was held in Paris. On that occasion, the main principles on which national protection enhancement policies should be based were identified.

G8 countries, in order to favor international cooperation, also for the benefit of non-G8 countries, have established an International CIIP Directory which lists points of contacts and relevant facilities in
each member country dealing with CIIP-related issues.

The **European Commission** is currently looking into problems affecting research in Critical Infrastructure protection within the Sixth Framework Program, with respect to the IST (Information Society Technologies) priority and the Preparatory Action on Security Research.

### Sixth Framework Program

One of the three main technology sectors identified by the European Commission in the IST field is mobile, wireless, optic and broadband communications as well as software and information technologies that are reliable, pervasive, interoperable and adaptable to new applications and services.

Within the IST Priority, one of the strategic targets which had been indicated was that of directing research “towards a framework of global reliability and security”.

Among other things, the Commission wishes to develop tools to support decision-making, aimed at protecting critical infrastructures, preventing threats and reducing vulnerability considering ICT interdependence.

Already in the Fifth Framework Program, always within the IST priority, the European Commission had looked into research problems related to critical infrastructures with great attention.

The result of this activity was the **European Dependability Initiative** (DEPPY - http://deppy.jrc.it/default/). DEPPY launched a number of R&D projects on the “dependability” of Information Society systems and services and, more recently, on risk and vulnerability analyses on critical information infrastructures and their interdependence with other critical infrastructures; furthermore, it also fostered international cooperation by establishing the **EU-US Joint Task Force on R&D on CIP**.

Other important initiatives include the DDSI (http://www.ddsi.org/DDSI-F/main-fs.htm) and ACIP (www.iabg.de/acip/index.html) projects, which have contributed to
the definition of research priorities on the security and dependability of major information infrastructures.

Particularly interesting are the SecurIST and CI2RCO coordinated actions which are meant to identify research strategies on information system and infrastructure security.

**Preparatory Action on Security Research**

In 2004 the Commission, prompted by the European Parliament, Council and industry, has launched a preparatory action on security research in order to launch a global program after 2007.

The Preparatory Action is one of the Commission’s contributions to the broader EU agenda on how to face challenges and threats to Europe, which is also illustrated in the European Security Strategy which was approved by the Council in December 2003.

The European Commission has identified five “missions” related to protection against terrorist attacks, one of which is focused on research on critical infrastructures.

The name of the mission is «Optimizing security and protection of networked systems” and its purpose is to analyze, under the security viewpoint, present and future networked systems such as communication systems, utilities, transport infrastructures, (electronic) commerce and business networks, examining their vulnerabilities and interdependencies to highlight security options against both electronic and physical threats.

Priorities within this mission are the following:

- developing standardized methodologies and decision-making tools to assess the nature of potential threats and identify vulnerabilities;

- testing protection and security measures for critical elements in private, public and government infrastructures in the broader European Union;

- Developing detection, prevention, response and warning
capabilities to strengthen information and control systems, integrating the use of satellite and land-based wireless systems.

• At political and regulatory level, since 2001 the Commission has started working on a European approach to information and network security which led to the establishment of the **European Network & Information Security Agency (ENISA)** in November 2003.

**ENISA**

The Agency’s mission is to contribute in ensuring high security level for EU information networks and foster a culture of information and network security by empowering and involving all players – economic and industrial sectors, connectivity service providers, government agencies – so that they introduce security technologies, standards and good practices.

At operational level, the Commission has promoted the [eEurope 2005](http://europa.eu.int/information_society/eeurope/2005/index_en.htm) action plan; such plan, which replaces the eEurope 2002 action plan, is based on two categories of actions which mutually enhance each other: on the one hand, stimulating services, applications and contents for both public on-line services and e-business services; on the other hand, supporting and establishing a broadband basic infrastructure and carefully considering all security-related aspects.

**NATO**

**NATO** has been analyzing the issue of Critical Infrastructure Protection ever since 1997 within the Information Operation (IO) initiative. This problem was recently examined also in connection to Civil Defense and terrorism and a road-map was developed to favor a bet-
ter understanding of the problem and introduce adequate training, international cooperation and R&D initiatives.

UN

The United Nations (UN) repeatedly emphasized the importance of implementing policies aimed at improving information infrastructure security.

Critical infrastructure protection was specifically addressed during the 78th General Assembly which, in December 2003, adopted Resolution n.58 on the Creation of a global culture of cybersecurity and the protection of critical information infrastructures.

This resolution, in acknowledging that critical infrastructures are becoming ever more interdependent also due to the increasing spread of information infrastructures, shows how this might lead to a greater vulnerability for the entire system. This, in turn, leads to the need to implement actions aimed at reducing vulnerabilities and threats, minimizing possible damage and favoring recovery actions, also by providing better training to employees. In particular, the resolution invites member States to consider, in the definition of their strategies, the «Elements for protecting critical information infrastructures» which are attached the resolution and which are basically the same as the principles which were laid down in March 2003 by the G8.

OECD and UN documents

The documentation issued by the Organization for Economic Cooperation and Development (OECD in English, OCDE in French) is considered as a highly valuable reference source, both under the social and ethical viewpoint, also because it is often referred to by EU regulatory bodies.

will be summarized in this section, is particularly relevant.

Under the common denominator of promoting a culture of security, nine principles are identified:

1. **Awareness-raising** – Interested parties must be aware of the need to **protect information systems and networks**, and of the actions they might undertake to enhance security.

2. **Responsibility** – Interested parties are responsible for **information system and network security**.

3. **Response** – Interested parties must act promptly and in a spirit of cooperation in order to prevent, identify and respond to security incidents.

4. **Ethics** – Interested parties must respect other parties’ legitimate interests.

5. **Democracy** – **Information system and network security** must be compatible with democratic society’s fundamental values.


7. **Security Awareness and Implementation** – Interested parties must integrate security as an essential element of **information systems and networks**.

8. **Security management** – Interested parties must adopt a global approach to security management.

9. **Security redefinition** – Interested parties must examine and redefine their information system and network security and introduce appropriate changes to their security policies, actions and procedures.

Along the same lines of the OECD document, is the UN Resolution A/RES/58/199 of December 23, 2003 entitled “Creation of a global culture of cyber-security and the protection of critical information infrastructures”.

This resolution invites member States to consider eleven security principles, which are essentially based on the G8 principles of...
March 2003.

Table 1, which was prepared by the NISCC (National Infrastructure Security Coordination Centre), lists the principles laid down in the UN Resolution with reference to the OECD tenets which were described in the previous section. As you can see, compared to the OECD document, which was mostly addressed to society, providers and users (principles 2, 4 and 5), the UN resolution is more specifically targeted to Governments and law-enforcement agencies (principles 6, 7 and 9).

**EU Directives and other documents**

Over the last few years the Italian Government has promptly implemented the EU Directives on network and information security. The (Transport/Telecommunication) Council resolution of December 11, 2001 entitled «Resolution on network and information security» is particularly noteworthy in this respect. The document asked member States to perform the following actions by the end of 2002:

- Promoting a culture of security through **education campaigns** aimed at public administrations, businesses, ISPs etc.
- Promoting **best security practices** based on international standards, especially amongst SMEs.
- Promoting **security during IT courses**.
- Enhancing **computer emergency response teams**
- Promoting the knowledge and adoption of the **Common Criteria (CC) security standard** included in the ISO15408 standard.
- Promoting the study and adoption of **biometric devices**.
<table>
<thead>
<tr>
<th>Topics</th>
<th>Principles of UN Resolution 58/199</th>
<th>Reference to OECD principles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Warnings and reaction to accidents</strong></td>
<td>1. Having network facilities to issue warnings about information vulnerabilities, threats and accidents.</td>
<td>3. Response</td>
</tr>
<tr>
<td></td>
<td>5. Establishing and maintaining communication networks for crisis situations, testing them periodically to ensure their efficiency in times of emergency.</td>
<td></td>
</tr>
<tr>
<td><strong>Awareness-raising and training</strong></td>
<td>2. Raising awareness so that all interested parties can more easily appreciate the extent and nature of their critical information infrastructures and the role that each party has in their protection.</td>
<td>1. Awareness-raising</td>
</tr>
<tr>
<td></td>
<td>8. Organizing training initiatives and drills to increase responsiveness as well as testing continuity and crisis plans in case of attacks against information infrastructures, encouraging peers to carry out similar activities.</td>
<td></td>
</tr>
<tr>
<td><strong>Risk analysis</strong></td>
<td>3. Examining infrastructures to identify their interdependencies in order to improve their protection.</td>
<td>6. Risk assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. Security management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Security reassessment</td>
</tr>
<tr>
<td><strong>Security Technology</strong></td>
<td>11. Promoting national and international research and development and favoring the introduction of security technologies that are consistent with international standards.</td>
<td>7. Security awareness and implementation</td>
</tr>
<tr>
<td><strong>Information sharing and international cooperation</strong></td>
<td>10. Embarking upon appropriate international cooperation initiatives to enhance critical information system security, also through the development and coordination of warning and alert systems, through the sharing and dissemination of information regarding vulnerabilities, threats and accidents and coordinating investigations on attacks against information systems, in accordance with local legislation.</td>
<td>3. Response</td>
</tr>
<tr>
<td></td>
<td>4. Promoting cooperation between both private and public partners to share and analyze information referring to critical infrastructures in order to prevent, investigate on and react to attacks against infrastructures and possible damage.</td>
<td></td>
</tr>
<tr>
<td><strong>Legal and criminal investigation issues</strong></td>
<td>9. Having adequate laws, both under the formal and substantial viewpoint, and adequately trained staff to allow States to investigate and prosecute attacks against critical information systems and coordinate such activities with other States when necessary.</td>
<td>2. Responsibilities</td>
</tr>
<tr>
<td></td>
<td>6. Making sure that laws regarding data availability take into account the need to protect critical information systems.</td>
<td>4. Ethics</td>
</tr>
<tr>
<td></td>
<td>7. Facilitating the tracking down of attacks against critical information systems and, whenever appropriate, communicating information on such tracking activities to other States.</td>
<td>5. Democracy</td>
</tr>
</tbody>
</table>

Table 1: A comparison between the OECD document and the UN Resolution
Promoting information exchange and cooperation amongst member States.

Another very interesting document is the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions of June 2001 entitled “Network and Information Security: Proposals for a European Policy Approach”.

In this document, the various threats and attacks (known at the time, today some more should be added) against networks are analyzed, together with related remedies. It is a useful security planning document, which was taken into account in drafting the following paragraphs which are included in this section.

On July 12, 2002, the “EU Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector” was issued. This provision, which totally replaces the previous directive 97/66/EC, reflects the need for a legislative update following the evolution of technology, over five years, leading to greater risks of infringing user privacy. This provision, amongst other things, also introduces the terms electronic communication service and network following the convergence of voice and data communication services.

Such directive was broadly transposed, and came into force in Italy with the “Legislative Decree n. 196 of June 30, 2003 – Provisions concerning personal data protection”.

I – General Remarks
1.5 THE ITALIAN SITUATION

In May 2002, the Ministerial Commission for Information Society prepared a document called “Government Guidelines for the Development of the Information Society” which was published by the Innovation and Technology Ministry.

The Guidelines describe and identify the Government’s commitment to turn Italy into a key global player in the digital era, modernizing the country through the widespread use of new ICTs both in the public and private sector.

However, an increase in traffic also requires an equal increase in secure network usage, as well as the establishment of a security model that is able to bring citizens and businesses closer to the network, especially in their relations with the public administration.

The problem of network security is also envisaged in the Guidelines and a national plan for ICT security and privacy is introduced.

The document identifies five main actions on which the general national strategy for ICT security should be founded:

Transposition of the Directive on ICT security: this directive defines a “Minimum Security Base” that all Administrations must comply with, once they have assessed their own ICT security level.

Establishment of a National Technical Committee on ICT security: The Committee is made up of five experts who are tasked with guiding and coordinating all relevant activities and efforts aimed

---


4 INTERMINISTERIAL DECREE ISSUED BY THE COMMUNICATION MINISTER AND THE INNOVATION AND TECHNOLOGY MINISTER - «Establishment of the National Technical Committee on Information and Telecommunication Security in Public Administration».
at defining a National Security Model and then introduce all technical and organizational measures which are needed for its implementation. The committee’s composition and activity is based on the total collaboration between the Communication Ministry and the Department for Innovation and Technology.

Establishment of a national structure of ICT security facilities and responsibilities, which is able to develop guidelines, recommendations, standards and certification procedures.

Introduction of a National Information Security Plan defining activities, responsibilities, and timing for the introduction of necessary standards and methodologies for security certification in the Public Administration.

In March 2003, the Innovation and Technology Ministry established the Working Group on CIIP, in which representatives from ministries involved in critical infrastructure management (Interior, Infrastructure, Communication Ministries, etc.), major private providers (ABI, ASI, CESI, GRTN, RFI, Snam Rete Gas, Telecom Italia, Wind and others) and the research and academic world took part.

The Working Group’s main aim was to help institutions to better understand problems associated to CIIPs and provide basic indications to identify organizational requirements to enhance critical infrastructure robustness.

In March 2004, the Working Group on CIIP issued the document entitled Critical Information Infrastructure Protection – The Italian Situation in which the results of work carried out during the previous year are reported. The document analyzes the Italian situation with respect to the most important CNIs, emphasizing how their growing complexity and the need to provide innovative and high-quality services mandates the use of ICT and this, together with the dismantlement of old monopolies, contributes to increasing interdependencies between different infrastructures.

The Working Group, without questioning the prevention, protection and security responsibilities belonging to every provider in their respective area of activity based on the indications and directives
coming from technological evolution and existing legislation, underlines the need to consider also those variables that are not under the direct control of any singular provider, but for which it is necessary to develop joint risk management policies. Adopting such strategies depends upon a steady and proactive collaboration between different relevant public institutions and private providers.

The Interior Ministry, through the Postal and Communication Police, has launched specific initiatives to enhance security within information infrastructures used by CNIs and to facilitate repression activities against possible crimes in this field. These initiatives stem from the awareness of possible large-scale effects coming from criminal actions against critical infrastructures, hence the need to establish communication channels and effective information exchange with the different subjects involved. For this purpose, the Postal and Communication Police is signing agreements with various providers to define appropriate protocols for communication and information exchange.

1.5.1 Specific Activities for Network Security

Upon request of the Prime Minister's Office, the Superior Institute for ICT established the Security Certification Body for Commercial Information Systems and Products (Organismo di Certificazione della sicurezza dei sistemi e prodotti informatici commerciali - OCSI). This certification body allows for ICT security certification for ICT products/systems in accordance with Common Criteria and ITSEC standards. OCSI is working on specific programs for critical system assessment and certification and will be involved in disseminating ICT security certifications and culture in every field (public administration, SMEs, residential users, critical infrastructures, etc.).
1 – General Remarks

1.1 INTRODUCTION

The development and organization of industrialized countries are based on increasingly complex infrastructure systems: the so-called Critical National Infrastructures (CNI). They are defined as any public or private infrastructure whose operation is essential for a country’s security and functioning.

Such infrastructures oversee fundamental sectors for modern societies such as health care, the economy, energy, transport and communication systems, law enforcement, defense and, in general, public administration.

They can be affected by critical events of different nature, which are able to jeopardize their efficiency both directly and indirectly. Generally speaking, critical events are usually related to intentional attacks or natural disasters.

In order to work, CNIs increasingly rely on TLC infrastructures. (CII - Critical Information Infrastructures). These networks must guarantee CNIs’ operational viability under normal working conditions, but especially and more importantly when critical events occur.

However, critical events might not only involve CNIs, but also their related TLC infrastructures.

Furthermore, both CNIs and CIIIs might be subject to failures which are not caused by external events.
In this context, we shall refer to Critical Information Infrastructures (CII) as those Critical National Infrastructures which totally or partially rely on one or more information infrastructures\(^1\) for their monitoring, control and management.

Such information infrastructures must allow CNIs to operate under normal working conditions and they should also guarantee a commensurate operative capability in case of an emergency, that is when critical events occur.

We should not even underestimate the high degree of interdependence existing between several Critical Infrastructures. As a matter of fact, at a very high level, it is possible to provide a hierarchical description of the interdependence existing between different sectors as follows (Fig. 1):

\[\text{NETWORK SECURITY}\]
\[\text{in critical infrastructures}\]

\(^1\) In literature, the CII acronym also refers to “Critical Information Infrastructures”, giving greater importance to protection aspects specific to the cyberspace and in particular Internet.
As it might be observed, the highest ranking factor is Country: the regular development of a Nation’s economic and social life strongly depends upon the quality of a number of underlying essential services.

In a nutshell, the most important pillars are Energy and TLC (and related IT), as well as “value-added” services such as Health Care, Civil Defense, and so forth, which anyhow rely on the first two pillars.

By definition, Energy is the element without which no job can be done. Therefore, any advanced service depends upon a proper energy production, transmission and distribution.

TLC and IT are the elements without which no signal, data or information transmission is possible and hence, the appropriate coordination of both local and remote (human and technological) resources is not possible either.

However, Energy and Telecommunications are mutually interdependent: without adequate and steady power supply, ICT equipment cannot work and power production, transmission and distribution grids can work only if communication systems are able to connect different facilities.

More specifically, the aim of this document is to provide a number of initial proposals concerning critical issues related to the interdependence existing between traditional CNI and TLC infrastructures, including also Information and TLC networks proper.

Document aim is to provide CNIs with basic indications on how to adequately set up their communication systems, in order to guarantee the necessary effectiveness also in emergency situations.

1.2 CNI AND CII: INTERDEPENDENCE AND PROTECTION

CNIs, despite the specificities deriving from their respective tasks, share a number of common features:

- They are all widely distributed throughout the national territory
- High visibility
- Difficulties in keeping all facilities under surveillance
- Potential coordination and intercommunication problems

• They all have a public service mission
  - Severe availability and reliability requirements
  - Rapid reaction and recovery characteristics in times of crisis
  - Infrastructures characterized by maximum resilience and security
  - Potential repercussions on public safety

• They must provide for interoperability with external public and private users/clients.
  - High intrusion risk
  - They require controlled and secure access points for multi-protocol communications
  - Important economic consequences due to failures/sabotage.

Critical national infrastructures include the following:

• Energy transmission and distribution networks (electricity, gas, etc.)
• TLC networks
• Transport systems (goods and passengers)
• Emergency services
• Defense infrastructures
• Banking and financial circuits
• National health care services
• Water transport, distribution and treatment systems
• Media and public information networks
• Farming and food processing industries
• Government networks
Several events might totally or partially affect infrastructure efficiency in one or more Countries: natural events (floods, earthquakes, volcanic eruptions), events caused by voluntary (terrorism, cyber-crime) or involuntary (errors, omissions) human actions, events affecting the environment (pollution, chemical substances, fires), events related to equipment malfunctions (hardware failures, software bugs, etc.).

The recent report published by the Canadian government on the security of its CNIs [8] shows that over the next few years the scenario will be characterized by a remarkable increase in the number of threats related to natural events (due to extreme climate changes) and criminal actions (linked to the current social and political context, especially terrorism).

This last aspect is related to a number of independent causes which, unfortunately, are also concurrent. On the one hand, the spread and importance of IT at all levels of CNI management and control is such that they have become privileged targets for both traditional criminal activities and cyber-crime. Hence, CNIs must take into account, in addition to “traditional” physical threats, also those threats which might directly or indirectly exploit information technology.

By the same token, increased terrorist threats must be considered also, which might target CNIs to wreak havoc in several countries and cause uncertainty amongst their citizens. Terrorist activities which might only be limited to providing “support” to other kinds of criminal actions in order to enhance their effect and/or delay rescue and recovery operations, thereby magnifying their media impact.

As was already underlined in the document entitled “CII Protection – The Italian Situation”\textsuperscript{2}, in addition to threats we also have to remember that the CNIs’ architectural scenario is changing rapidly and profoundly.

\textsuperscript{2} Written in March 2004 by the working group established by the Department for Innovation and Technology of the Prime Minister’s Office
As a matter of fact, “up to ten years ago, each of these infrastructures could be considered as a substantially independent and self-sufficient system, managed by vertically integrated operators. For a number of reasons, the structure has gone through a profound change so that now all infrastructures tend to be interdependent, especially since they now share the so-called cyberspace, i.e. the virtual space produced by the interconnection of computers, telecommunication systems, application and data. Therefore, any (accidental or willfully caused) failure in any infrastructure can easily extend to other infrastructures, according to a domino effect, magnifying its effects and causing malfunctions and dysfunctions also to users who are quite remote, both geographically and functionally, from the place where the initial failure occurred". [1]

The power failure which affected most of the US North-East coast in August 2003 is a remarkable example of how a simple malfunction in a few modules of a distribution company’s IT control system, joined with a number of other accidental events, might lead to the almost complete paralysis of all local infrastructures causing billions of dollars in damage.

This is also due to the fact that, following the widespread use of Information Society technologies, Critical Infrastructures have developed a growing interdependence whereby events happening in one specific sector might have an immediate impact on all others. In particular, natural events or criminal actions affecting one CNI, lead to a multiplication and magnification of effects so that even minor events might cause serious and widespread damage.

Therefore, the current scenario is characterized by both greater and more diversified threats against CNIs, as well as by a different infrastructural context which, because of existing interdependencies, engenders a new kind of vulnerability. This requires a greater and different attention towards all aspects related to each individual CNI’s protection, security and robustness, in order to protect national CNIs.

This infrastructural scenario is also going through deep change: infrastructures are now expected to provide innovative and extremely high quality services while, at the same time, preserving their efficiency and cost-effectiveness. This requires the best possible use of each country’s technology infrastructures which can only be achieved
through the massive introduction of advanced automatic control systems and, more in general, through the use of ICT.

In order to better understand the crucial role played by all aspects related to ICT security for critical infrastructure protection, it is useful to refer to the diagram in Fig. 2. Every CNI can be described as a complex structure built over physical, cyber, organizational and strategic layers. Within each CNI, functional links exist between different layers and, at the same time, dependence and interdependence relations exist between the corresponding layers belonging to different CNIs.

Figure 2: Multi-layer infrastructural model, developed by ENEA for the Safeguard European project.
The widespread use of ICT has led to an ever increasing importance of both the cyber-layer within each infrastructure and of the interdependencies existing between the same layers in different infrastructures.

We must point out that, in this context, the term cyber-layer does not correspond to corporate information systems but, rather, to that part within these systems which is entrusted with managing and controlling the infrastructure’s physical layer.

In this framework, as can be seen in Fig. 3, within the broader issue of Critical Infrastructure Protection – CIP, the protection of such “Control and Supervision” layer is what is commonly indicated as Critical Information Infrastructure Protection – CIIP.

Within Critical Infrastructure Protection strategies, CIIP has become a central and increasingly important element.

The term CIIP (Critical Information Infrastructure Protection) refers to all those actions that are meant to enhance security, reliability and appropriate operation for all those critical infrastructures which totally or partially use any information infrastructure for monitoring, management or control purposes.

Figure 3: Scope of CIP and CIIP definitions [CiSP]
Therefore, if we go back to the definition laid down in [1], we can say that CIIP includes all those actions that are meant to enhance security, reliability and availability for all those critical infrastructures which totally or partially use any information infrastructure for monitoring, management or control purposes.

Such initiatives are not limited to the IT security of the cyber-layer, but include all aspects related to service continuity and regularity.

### 1.3 AIMS OF THIS BOOK AND WORKING GROUP ACTIVITIES

This Report summarizes work carried out in March 2004 by the Working Group which was established within the Communication Ministry.

The Working Group, made up by representatives of the most important public administrations, together with representatives coming from some of the main Italian CNI operators and specialized Companies in this field, focused on the role played by TLC infrastructures with respect to CNI security and service continuity.

The Working Group, benefiting from each member’s expertise, has tried to bring together needs and possible solutions, in order to provide CNI managers with guidelines, or best practices, which might lead to greater effectiveness and awareness in the use of necessary and existing communication systems.

The Working Group analyzed the following aspects:

- Quality of Service and TLC Network Security, also considering International and National Reference Standards and Legislation;

- problems caused by interdependence between CNIs and between CNIs and TLC infrastructures;

- identifying main threats against TLC infrastructures used by CNIs;
• identifying a minimum set of security parameters in order to qualify the security status of TLC infrastructures supporting CNIs;

• identifying minimum technical parameters to guarantee adequate Quality of Service (QoS) providing for the least possible critical situations;

• identifying a number of technical parameters, transparency elements and legal terms which should be used in commercial contract relations and in Service Level Agreements (SLAs) signed with TLC service Providers;

• potential roles Institutions might play to identify and implement common protection strategies;

• Some proposals to self-assess current vulnerability and organization statuses within each CNI.

The following aspects were not considered:

• problems referring to critical components that are not IT-based, are not involved in TLC activities, are peculiar to each CNI (e.g. water or gas distribution systems) and might lead to total failure in case of failure or attack;

• Security issues related to Platforms and Management Applications used by Companies who own CNIs, but that are not directly linked to critical component management (e.g. ERP, payroll systems, database, etc.).
1.4 CURRENT INTERNATIONAL INITIATIVES FOR CII PROTECTION

The first studies on security and service continuity problems for critical information infrastructures were started in the 1990s.

The US was the first country to think about specific government actions on this issue which, in 1998, resulted in the issuance of Presidential Decision Directives 62 and 63.

Since then, several other industrialized countries have developed actions aimed at:

- understanding critical and vulnerable elements of each country’s critical infrastructures, highlighting their weaknesses;
- laying down strategies to mitigate such weaknesses;
- raising awareness amongst service providers on the issue of critical infrastructure protection;
- developing emergency and recovery plans to be implemented in case of negative events affecting one or more critical infrastructures;
- supporting the development of inherently secure technologies;
- Supporting international cooperation.

The issue of Critical Information Infrastructure protection, due to its transnational scope, was recently submitted to the attention of several international institutions.

In March 2003, the first meeting of G8 country experts on CIIP was held in Paris. On that occasion, the main principles on which national protection enhancement policies should be based were identified.

G8 countries, in order to favor international cooperation, also for the benefit of non-G8 countries, have established an International CIIP Directory which lists points of contacts and relevant facilities in...
each member country dealing with CIIP-related issues.

The European Commission is currently looking into problems affecting research in Critical Infrastructure protection within the Sixth Framework Program, with respect to the IST (Information Society Technologies) priority and the Preparatory Action on Security Research.

**Sixth Framework Program**

One of the three main technology sectors identified by the European Commission in the IST field is mobile, wireless, optic and broadband communications as well as software and information technologies that are reliable, pervasive, interoperable and adaptable to new applications and services.

Within the IST Priority, one of the strategic targets which had been indicated was that of directing research “towards a framework of global reliability and security”.

Among other things, the Commission wishes to develop tools to support decision-making, aimed at protecting critical infrastructures, preventing threats and reducing vulnerability considering ICT interdependence.

Already in the Fifth Framework Program, always within the IST priority, the European Commission had looked into research problems related to critical infrastructures with great attention.

The result of this activity was the European Dependability Initiative (DEPPY - http://deppy.jrc.it/default/). DEPPY launched a number of R&D projects on the “dependability” of Information Society systems and services and, more recently, on risk and vulnerability analyses on critical information infrastructures and their interdependence with other critical infrastructures; furthermore, it also fostered international cooperation by establishing the EU-US Joint Task Force on R&D on CIP.

Other important initiatives include the DDSI (http://www.ddsi.org/DDSI-F/main-fs.htm) and ACIP (www.iabg.de/acip/index.html) projects, which have contributed to
the definition of research priorities on the security and dependability of major information infrastructures.

Particularly interesting are the SecurIST and CI2RCO coordinated actions which are meant to identify research strategies on information system and infrastructure security.

**Preparatory Action on Security Research**

In 2004 the Commission, prompted by the European Parliament, Council and industry, has launched a preparatory action on security research in order to launch a global program after 2007.

The Preparatory Action is one of the Commission’s contributions to the broader EU agenda on how to face challenges and threats to Europe, which is also illustrated in the European Security Strategy which was approved by the Council in December 2003.

The European Commission has identified five “missions” related to protection against terrorist attacks, one of which is focused on research on critical infrastructures.

The name of the mission is «Optimizing security and protection of networked systems” and its purpose is to analyze, under the security viewpoint, present and future networked systems such as communication systems, utilities, transport infrastructures, (electronic) commerce and business networks, examining their vulnerabilities and interdependencies to highlight security options against both electronic and physical threats.

Priorities within this mission are the following:

- developing standardized methodologies and decision-making tools to assess the nature of potential threats and identify vulnerabilities;
- testing protection and security measures for critical elements in private, public and government infrastructures in the broader European Union;
- Developing detection, prevention, response and warning
capabilities to strengthen information and control systems, integrating the use of satellite and land-based wireless systems.

• At political and regulatory level, since 2001 the Commission has started working on a European approach to information and network security which led to the establishment of the European Network & Information Security Agency (ENISA) in November 2003.

ENISA

The Agency’s mission is to contribute in ensuring high security level for EU information networks and foster a culture of information and network security by empowering and involving all players – economic and industrial sectors, connectivity service providers, government agencies – so that they introduce security technologies, standards and good practices.

At operational level, the Commission has promoted the eEurope 2005 action plan (http://europa.eu.int/information_society/eeurope/2005/index_en.htm); such plan, which replaces the eEurope 2002 action plan, is based on two categories of actions which mutually enhance each other: on the one hand, stimulating services, applications and contents for both public on-line services and e-business services; on the other hand, supporting and establishing a broadband basic infrastructure and carefully considering all security-related aspects.

NATO

NATO has been analyzing the issue of Critical Infrastructure Protection ever since 1997 within the Information Operation (IO) initiative. This problem was recently examined also in connection to Civil Defense and terrorism and a road-map was developed to favor a bet-
ter understanding of the problem and introduce adequate training, international cooperation and R&D initiatives.

**UN**

The United Nations (UN) repeatedly emphasized the importance of implementing policies aimed at improving information infrastructure security.

Critical infrastructure protection was specifically addressed during the 78th General Assembly which, in December 2003, adopted Resolution n.58 on the Creation of a global culture of cybersecurity and the protection of critical information infrastructures.

This resolution, in acknowledging that critical infrastructures are becoming ever more interdependent also due to the increasing spread of information infrastructures, shows how this might lead to a greater vulnerability for the entire system. This, in turn, leads to the need to implement actions aimed at reducing vulnerabilities and threats, minimizing possible damage and favoring recovery actions, also by providing better training to employees. In particular, the resolution invites member States to consider, in the definition of their strategies, the «Elements for protecting critical information infrastructures» which are attached the resolution and which are basically the same as the principles which were laid down in March 2003 by the G8.

**OECD and UN documents**

The documentation issued by the Organization for Economic Cooperation and Development (OECD in English, OCDE in French) is considered as a highly valuable reference source, both under the social and ethical viewpoint, also because it is often referred to by EU regulatory bodies.

will be summarized in this section, is particularly relevant.

Under the common denominator of promoting a culture of security, nine principles are identified:

1. **Awareness-raising** – Interested parties must be aware of the need to **protect information systems and networks**, and of the actions they might undertake to enhance security.

2. **Responsibility** – Interested parties are responsible for **information system and network security**.

3. **Response** – Interested parties must act promptly and in a spirit of cooperation in order to prevent, identify and respond to security incidents.

4. **Ethics** – Interested parties must respect other parties’ legitimate interests.

5. **Democracy** – **Information system and network security** must be compatible with democratic society’s fundamental values.


7. **Security Awareness and Implementation** – Interested parties must integrate security as an essential element of **information systems and networks**.

8. **Security management** – Interested parties must adopt a global approach to security management.

9. **Security redefinition** – Interested parties must examine and redefine their information system and network security and introduce appropriate changes to their security policies, actions and procedures.

Along the same lines of the OECD document, is the UN Resolution A/RES/58/199 of December 23, 2003 entitled “Creation of a global culture of cyber-security and the protection of critical information infrastructures».

This resolution invites member States to consider eleven security principles, which are essentially based on the G8 principles of
March 2003.

Table 1, which was prepared by the NISCC (National Infrastructure Security Coordination Centre), lists the principles laid down in the UN Resolution with reference to the OECD tenets which were described in the previous section. As you can see, compared to the OECD document, which was mostly addressed to society, providers and users (principles 2, 4 and 5), the UN resolution is more specifically targeted to Governments and law-enforcement agencies (principles 6, 7 and 9).

EU Directives and other documents

Over the last few years the Italian Government has promptly implemented the EU Directives on network and information security. The (Transport/Telecommunication) Council resolution of December 11, 2001 entitled «Resolution on network and information security» is particularly noteworthy in this respect. The document asked member States to perform the following actions by the end of 2002:

• Promoting a culture of security through education campaigns aimed at public administrations, businesses, ISPs etc.

• Promoting best security practices based on international standards, especially amongst SMEs.

• Promoting security during IT courses.

• Enhancing computer emergency response teams

• Promoting the knowledge and adoption of the Common Criteria (CC) security standard included in the ISO15408 standard.

• Promoting the study and adoption of biometric devices.
### Table 1: A comparison between the OECD document and the UN Resolution

<table>
<thead>
<tr>
<th>Topics</th>
<th>Principles of UN Resolution 58/199</th>
<th>Reference to OECD principles</th>
</tr>
</thead>
</table>
| **Warnings and reaction to accidents** | 1. Having network facilities to issue warnings about information vulnerabilities, threats and accidents.  
5. Establishing and maintaining communication networks for crisis situations, testing them periodically to ensure their efficiency in times of emergency. | 3. Response                 |
| **Awareness-raising and training** | 2. Raising awareness so that all interested parties can more easily appreciate the extent and nature of their critical information infrastructures and the role that each party has in their protection.  
8. Organizing training initiatives and drills to increase responsiveness as well as testing continuity and crisis plans in case of attacks against information infrastructures, encouraging peers to carry out similar activities. | 1. Awareness-raising         |
| **Risk analysis**             | 3. Examining infrastructures to identify their interdependencies in order to improve their protection. | 6. Risk assessment           |
| **Security Technology**       | 11. Promoting national and international research and development and favoring the introduction of security technologies that are consistent with international standards. | 7. Security awareness and implementation |
| **Information sharing and international cooperation** | 10. Embarking upon appropriate international cooperation initiatives to enhance critical information system security, also through the development and coordination of warning and alert systems, through the sharing and dissemination of information regarding vulnerabilities, threats and accidents and coordinating investigations on attacks against information systems, in accordance with local legislation.  
4. Promoting cooperation between both private and public partners to share and analyze information referring to critical infrastructures in order to prevent, investigate on and react to attacks against infrastructures and possible damage. | 3. Response                  |
| **Legal and criminal investigation issues** | 9. Having adequate laws, both under the formal and substantial viewpoint, and adequately trained staff to allow States to investigate and prosecute attacks against critical information systems and coordinate such activities with other States when necessary.  
6. Making sure that laws regarding data availability take into account the need to protect critical information systems.  
7. Facilitating the tracking down of attacks against critical information systems and, whenever appropriate, communicating information on such tracking activities to other States. | 2. Responsibilities          |
| **Social and political considerations** |                                                                                                      | 4. Ethics                     |
|                               |                                                                                                                                                         | 5. Democracy                  |

"Network Security in Critical Infrastructures"
Promoting information exchange and cooperation amongst member States.

Another very interesting document is the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions of June 2001 entitled «Network and Information Security: Proposals for a European Policy Approach».

In this document, the various threats and attacks (known at the time, today some more should be added) against networks are analyzed, together with related remedies. It is a useful security planning document, which was taken into account in drafting the following paragraphs which are included in this section.

On July 12, 2002, the «EU Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector» was issued. This provision, which totally replaces the previous directive 97/66/EC, reflects the need for a legislative update following the evolution of technology, over five years, leading to greater risks of infringing user privacy. This provision, amongst other things, also introduces the terms electronic communication service and network following the convergence of voice and data communication services.

Such directive was broadly transposed, and came into force in Italy with the “Legislative Decree n. 196 of June 30, 2003 – Provisions concerning personal data protection». 
1.5 THE ITALIAN SITUATION

In May 2002, the Ministerial Commission for Information Society prepared a document called “Government Guidelines for the Development of the Information Society” which was published by the Innovation and Technology Ministry.

The Guidelines describe and identify the Government’s commitment to turn Italy into a key global player in the digital era, modernizing the country through the widespread use of new ICTs both in the public and private sector.

However, an increase in traffic also requires an equal increase in secure network usage, as well as the establishment of a security model that is able to bring citizens and businesses closer to the network, especially in their relations with the public administration.

The problem of network security is also envisaged in the Guidelines and a national plan for ICT security and privacy is introduced.

The document identifies five main actions on which the general national strategy for ICT security should be founded:

Transposition of the Directive on ICT security\(^3\): this directive defines a “Minimum Security Base” that all Administrations must comply with, once they have assessed their own ICT security level.

Establishment of a National Technical Committee on ICT security\(^4\): The Committee is made up of five experts who are tasked with guiding and coordinating all relevant activities and efforts aimed

\(^3\) DIRECTIVE OF THE PRIME MINISTER OF JANUARY 16, 2002 – DEPARTMENT FOR INNOVATION AND TECHNOLOGY. Published in the Official Gazette n.69 on March 22, 2002 - «Information and Telecommunication Security in State Public Administration

\(^4\) INTERMINISTERIAL DECREE ISSUED BY THE COMMUNICATION MINISTER AND THE INNOVATION AND TECHNOLOGY MINISTER - «Establishment of the National Technical Committee on Information and Telecommunication Security in Public Administration». 
at defining a National Security Model and then introduce all technical and organizational measures which are needed for its implementation. The committee’s composition and activity is based on the total collaboration between the Communication Ministry and the Department for Innovation and Technology.

Establishment of a national structure of ICT security facilities and responsibilities, which is able to develop guidelines, recommendations, standards and certification procedures.

Introduction of a National Information Security Plan defining activities, responsibilities, and timing for the introduction of necessary standards and methodologies for security certification in the Public Administration.

In March 2003, the Innovation and Technology Ministry established the Working Group on CIIP, in which representatives from ministries involved in critical infrastructure management (Interior, Infrastructure, Communication Ministries, etc.), major private providers (ABI, ASI, CESI, GRTN, RFI, Snam Rete Gas, Telecom Italia, Wind and others) and the research and academic world took part.

The Working Group’s main aim was to help institutions to better understand problems associated to CIIPs and provide basic indications to identify organizational requirements to enhance critical infrastructure robustness.

In March 2004, the Working Group on CIIP issued the document entitled Critical Information Infrastructure Protection – The Italian Situation in which the results of work carried out during the previous year are reported. The document analyzes the Italian situation with respect to the most important CNIs, emphasizing how their growing complexity and the need to provide innovative and high-quality services mandates the use of ICT and this, together with the dismantlement of old monopolies, contributes to increasing interdependencies between different infrastructures.

The Working Group, without questioning the prevention, protection and security responsibilities belonging to every provider in their respective area of activity based on the indications and directives
coming from technological evolution and existing legislation, under-
lines the need to consider also those variables that are not under the
direct control of any singular provider, but for which it is necessary to
develop joint risk management policies. Adopting such strategies
depends upon a steady and proactive collaboration between different
relevant public institutions and private providers.

The Interior Ministry, through the Postal and Communication
Police, has launched specific initiatives to enhance security within
information infrastructures used by CNIs and to facilitate repression
activities against possible crimes in this field. These initiatives stem
from the awareness of possible large-scale effects coming from crim-
inal actions against critical infrastructures, hence the need to establish
communication channels and effective information exchange with the
different subjects involved. For this purpose, the Postal and
Communication Police is signing agreements with various providers to
define appropriate protocols for communication and information
exchange.

1.5.1 Specific Activities for Network Security

Upon request of the Prime Minister’s Office, the Superior
Institute for ICT established the Security Certification Body for
Commercial Information Systems and Products (Organismo di
Certificazione della sicurezza dei sistemi e prodotti informatici com-
merciali - OCSI). This certification body allows for ICT security certi-
fication for ICT products/systems in accordance with Common
Criteria and ITSEC standards. OCSI is working on specific programs
for critical system assessment and certification and will be involved in
disseminating ICT security certifications and culture in every field (pub-
lic administration, SMEs, residential users, critical infrastructures, etc.).
2.1 INTRODUCTION

This chapter deals with all aspects that have to be considered when critical infrastructures are to be analyzed.

We are referring to Critical National Infrastructure and, more specifically, to Critical National Information Infrastructure (CNII or CII).

With respect to CNII or CII, security problems deriving from critical infrastructure interdependencies and from specific threats affecting them are illustrated, suggesting a methodological approach for security management.

2.2 CRITICAL NATIONAL INFORMATION INFRASTRUCTURE PROTECTION

2.2.1 Technology Evolution and ICT Infrastructure Dependence

Evolutions in different markets are leading to substantial changes in our Country’s infrastructural set-up, which require innovative services that are also efficient and cheap.

This new context calls for the best possible use of technology infrastructures and this can be achieved only by introducing sophisti-
icated control mechanisms and using all kinds of information and communication technologies. Therefore CNI must consider, alongside “traditional” threats of a physical nature, also those threats which might be caused, directly or indirectly, by the use of Information Society technologies.

The transition is now being made from a situation where a number of substantially isolated, independent structures could be identified, managed by vertically integrated providers, to a situation which is characterized by widespread interdependence between different infrastructures due to the primary role played by ICT networks.

The establishment of these interdependencies is a new element of vulnerability for the entire Country, since technical failures, as well as targeted attacks against CNIs’ ICT systems, might have a negative impact on other Critical Infrastructures. They might cause dysfunctions and malfunctions which could be amplified to the extent that they might affect remote users (geographically or functionally) with respect to the place where the failure originally occurred.

In order to safeguard services provided by CNI, the appropriate functioning of Critical ICT Infrastructure (CII) must be ensured also in critical situations, for instance when the main power supply or intermediate links or equipments stop working, by including redundant components (power supply, equipment, routes, technology, installations etc.) within the general architecture, as well as prevention mechanisms against possible failures or malfunctions which might be determined, as we have already said, both by accidental and intentional causes.

For this reason, it is useful to wonder whether we ourselves or our providers know how resilient our ITC systems are in case of critical events, and what impact they might cause on the service we are supposed to guarantee.

First and foremost, this kind of awareness requires the knowledge of the tolerable degree of degradation (both in terms of time and performance) of one or more intermediate service elements (whether internal or external).

Tolerability (see Fig. 4) strictly depends upon two aspects:
countermeasure effectiveness and service performance degradation before the event becomes totally paralyzing. 

Appropriate temporary countermeasures must be envisaged to limit malfunctions within tolerability extremes (time and/or performance wise), and choose (internal or external) technology or service elements which can guarantee service discontinuities/degradation not exceeding the tolerability limit which has been identified.

For this purpose, it would be useful to draw up a table where technologies/services used for specific CNI operational capabilities can be cross-referenced, showing their critical level in guaranteeing CNIs’ regular operation and tolerability levels in case of failure.

Of course, every CNI would draw up that table differently and it would show not only the complex interdependence existing between different CNI and CII but also, and especially, that it is not possible to provide the same ICT service/infrastructure to meet all critical needs in every circumstance. Therefore, a thorough internal analysis must be carried out first, to be later extended to provider infrastructures and services, in order to setup a resilient architecture with respect to specific critical events and potential threats.

Figure 4: Malfuction tolerability
<table>
<thead>
<tr>
<th><strong>Function operated by TLC service in the CNI/Impact</strong></th>
<th><strong>TLC and similar services with critical level</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name of Function</strong></td>
<td><strong>TLC and similar services with critical level</strong></td>
</tr>
<tr>
<td>(Non CNI) External Communication</td>
<td>IP WAN/VPN</td>
</tr>
<tr>
<td>Communication with other CNI</td>
<td></td>
</tr>
<tr>
<td>Communication with other remote sites in the same CNI</td>
<td></td>
</tr>
<tr>
<td>Remote Equipment Monitoring</td>
<td></td>
</tr>
<tr>
<td>Other CNI-specific functions</td>
<td></td>
</tr>
</tbody>
</table>

**Table 2: Example of Correlation Table between Functions and Critical Services**

**DEFINITIONS**

"Critical Impact of function on CNI Mission" Specific function critical importance index with respect to CNI mission
1=low
2=critical but not paralyzing
3=paralyzing

"Tolerability time in case of interruption of specific service by provider" indication of the number of minutes/hours/days in which operation interruption due to serious TLC provider malfunction is tolerable
1=low critical relevance
2=critically relevant but not paralyzing
3=paralyzing

For every column of TLC services cross-referenced with each specific function:
0=not used
1=low critical relevance
2=critically relevant but not paralyzing
3=paralyzing
2.2.2 Security Issues in Critical Information Infrastructure

2.2.2.1 General Remarks

In the situation we described, it is necessary to implement a methodology which allows for a systematic analysis and reduction of risks deriving from new and broader threat and vulnerability scenarios and which, through the adoption of technical-organizational solutions, allows for greater survivability and protection for the entire Country System.

The aim is having an analysis methodology, which might apply in general to any System, which includes a number of solutions which can be both broadly applicable and specifiable to various contexts, that allows for:

- problem and risk situation definition
- identification of prevention actions in times of crisis
- identification of Crisis Management activities once a crisis is in progress.
- This model, due to the constant evolution of threats against CII, must envisage a constant and systematic risk assessment process.

2.2.2.2 Specific Critical Issues Associated to Critical Information Infrastructure

It is appropriate to make some comments about general issues associated to CII systems:

- With the extension of information networks and the widespread use of technology, the identification of actions and their correlation with the effects they produce has become ever more complex.
- Threats against CII systems have no geographical or political
boundaries and the constant extension of the global network makes tracking activities more complex and less reactive.

- The time it takes to identify vulnerabilities, exploit them and implement countermeasures is getting shorter.

- The technologies which are used to attack systems are widely available at decreasing costs and information on how to carry out attacks is more readily accessible.

- Attack methods have evolved in the same way as the systems they target, becoming increasingly automated and sophisticated.

- Each new project should go through risk analysis to identify the appropriate organizational and financial resources that are needed to ensure its security.

### 2.2.2.3 Interdependencies between Critical Information Infrastructures

Speaking of telecommunication networks, media convergence and, more specifically, the Internet, are leading to the creation of a global infrastructure. Unfortunately, this situation, by bringing together different infrastructures, increases the entire system’s vulnerability since any attack or accident affecting one infrastructure might easily spread over to others, causing problems and damage also to (geographically and logically) remote users from failure cause. In some cases, CII interdependence can stretch beyond national borders (just think about power grid interconnection).

Understanding how the correct functioning of a CII depends upon the others is an important step when security actions are being planned, since it allows to realize to what extent one single CII can independently provide for its own security and/or face emergency situations. There are at least three different kinds of CII interdependencies which can be identified:
• Operational interdependencies
• Logical interdependencies
• Geographical interdependencies.

Interdependencies existing between different CIIs are such
that the sharing of information amongst (public and private) facilities
in charge of their management is essential for the implementation of
effective protection systems.

2.2.2.3.1 Operative Interdependencies

This kind of interdependencies happens every time a CII’s
operation depends upon another CII’s operation.

For example, the operation of telecommunications networks
depends upon the availability of electricity and therefore upon the
operation of the CII which produces and distributes power. It must
point out that, in this specific case, interdependence is mutual, since
the operation of power grids also depends upon telecommunication
networks.

2.2.2.3.2 Logical Interdependencies

In some cases of attack or accident which jeopardize a CII’s
regular operation, this might lead to repercussions on other CIIs
although there might not be any operational interdependence between
them.

Just think about a localized epidemics which might cause a
health care system crisis also in areas which are at a great distance from
the affected region, due to the high number of people which might turn
to health care facilities even without any reason; or think about the pos-
sible transport system crisis in affected areas because travelers avoid
going there (e.g. the crisis which struck airlines in the US after 9/11).
2.2.2.3.3 Geographical Interdependencies

Geographical interdependencies between CIIs are completely different compared to the ones previously described. They happen every time critical elements for the regular operation of two or more CIIs share the same geographical location, irrespective of their nature.

This means that specific accidental events or deliberate attacks might jeopardize the ability of several CIIs to provide their services at the same time. Being aware of the existence of these kinds of interdependencies is very important during risk analysis, since it allows to avoid wrong statistical assumptions on the likelihood of some events happening.

2.2.2.4 Threats

2.2.2.4.1 Definition

Usually “threats” are associated to the ability, on the part of individuals or organizations, to strike at a critical infrastructure with the deliberate intent to jeopardize its operational capabilities.

However, in the broader context of CNI protection and security that we are considering here, we must remember that threats do not necessarily originate from human beings, but they might also have a natural or environmental origin.

Therefore, a “threat” can be defined as the potential capacity of an action or accidental event to cause damage by exploiting a specific vulnerability in the infrastructure which is being considered.

2.2.2.4.2 Classification

An initial classification of threat sources is the following:

- **Natural Sources**: they are associated to catastrophic events such as earthquakes, floods, volcanic eruptions, storms, avalanches and the like.
• **Human Sources**: they are associated to direct human actions which, in turn, might be subdivided into:
  - Involuntary or accidental actions (e.g. wrong data entry)
  - Voluntary actions (deliberate attacks against systems, unauthorized access to information, etc.)

• **Environmental Sources**: they are associated to a mixture of human actions and natural events such as pollution, fires, extended blackout, release of chemical substances or hazardous materials, etc.

• **Technological Sources**: they are associated to Hardware or Software component malfunctions or wrong configuration.

  All actions that are expected once threats do materialize have to be associated to the different threat sources.

  For threats deriving from voluntary human actions, the analysis will also have to consider those aspects which are related to the motivation behind a given threat.

  These analyses become particularly important for CII, where motivation and resources can substantially enhance the seriousness of the threat. For example:

  • A «hacker» might be motivated by a sense of challenge and will strive to penetrate into protected systems

  • A «Computer criminal» (or «cracker») will be interested in acquiring protected information or manipulating data and will target applications.

  • A terrorist will aim at causing maximum damage and might perpetrate both physical and virtual attacks to make the system unworkable.

  • An insider (within the organization) will act out of curiosity, to obtain advantages, out of revenge, or simply due to negligence or by mistake, thereby altering system functionalities.
As for CII, threats can be further classified depending on the kind of target that is considered:

- **Physical**: such as communication equipment or a simple interconnection cable.
- **Virtual**: such as data and information, or applications embedded in a CII.

In the same way, attacks can be identified depending upon the kinds of means being used:

- **Physical**: such as actions against physical targets (equipment or cable), or physical attacks against virtual targets (e.g. electronic jamming systems).
- **Virtual**: such as data destruction or manipulation or an equipment failure caused by actions against management systems.

### 2.2.3 Security Management

The first step when looking for a solution for Critical Infrastructure Protection is establishing a constant and systematic risk management process to identify, control and reduce risks and potential negative impacts which might derive from them.

It is essential for every CII to have a clear picture of their situation, also considering the use of common infrastructures and interdependencies with other CII, and establish an organizational infrastructure to implement all necessary processes to define, set up and maintain an effective security program.

This means defining appropriate methodological, information and organizational tools (procedures, operational flows, actions and communication methodologies involving entities entrusted with infrastructure security protection) to address CII protection in a systematic, conscious and reasoned way and guarantee the best possible crisis management when crises cannot be averted.
Bear in mind that, considering the close interdependence existing between various CNIs, the optimization of security resources requires a coordinated approach amongst CIIs and, hence, a high degree of awareness on their part concerning protection issues.

Therefore, a security management methodology must be identified (including risk analysis and management). In particular, this methodology will have to envisage the following stages:

1. identification and modeling of context to be protected
2. threat and vulnerability analysis
3. risk assessment
4. risk management strategy definition
5. choice effectiveness evaluation
6. operational procedure simulation and testing.

The risk management process is made up of a number of systematic activities which are periodically repeated in order to foster a security approach based on controllable and measurable elements which should not be linked, as far as possible, to subjective perceptions of risk or security needs. This process, in addition to provide guarantees about the effectiveness of possible protection measures, also facilitates an efficient allocation of resources assigned for Infrastructure protection.

### 2.2.3.1 Context Identification and Modeling

Identifying the context to be protected is the initial and fundamental stage of the entire security “planning” process. The ensuing risk analysis and the quality of achievable results both depend upon this step.
During this stage, the following actions must be carried out:

- identifying and listing the elements which make up the infrastructure that is being examined;
- identifying interdependencies existing between these elements and with elements which are part of other CII;
- establishing the critical level of the different elements with respect to the impact that their possible failure might have on CII operational continuity and to the side effects that such failure might have (in terms of direct and/or indirect economic losses or even risks for human beings).

The reality representation methodology which is used must allow for an accurate description of CNII and its interactions, using a model which is able to make the ensuing risk analysis easier. The choice of an appropriate level of detail is particularly important in order to describe and model reality in terms of so-called “Risk Units”, i.e. atomic elements (installations, people or even services, information, etc.) which have to be considered when describing relevant scenarios on which risk analysis will be carried out.

This methodology must have a broad application scope, since the identification of appropriate “Risk Units” can be made at the level of CNI. For example, if we consider the “Railway Transport” CNI, “risk units” could be: stations or parts of them; passengers; staff; trains; railway sections; control centers; baggage or goods storage facilities; etc.

By applying this methodology to specific CNII contexts, typical “risk units” might be identified such as, for example:

- sites where data processing centers or communication infrastructures are located;
- areas where ICT equipments are installed;
- relevant staff;
- control and management systems;
- power supply systems;
- communication networks and geographical connections used by infrastructure;
- etc.
Every “risk unit” will have to be associated to a number of descriptive attributes and other useful information (such as blueprints, images, descriptions, etc.). In the case of the Processing Center “unit risk”, for instance, these attributes might include (by way of example):

- site ID number;
- names of people in charge;
- IT center size and capacity;
- geographical location;
- economic value;
- strategic value;
- value in terms of image;
- etc.

“Risk units” will have to be assessed in relation to C.I.A. (confidentiality, integrity, availability) requirements based on qualitative or quantitative methods, in order to define their critical level.

There should also be the possibility to associate “risk units” to the following aspects, also considering dependencies existing with other CNI elements or other CNI:

- relevant threats;
- existing protection measures;
- detected vulnerabilities.

### 2.2.3.2 Threat, Impact and Vulnerability Analysis

The primary aims of this stage are the following:

- identifying possible threats against Critical Infrastructure and, more specifically, against its “risk units”;  
- defining the various threats in terms of:
  - expected frequency of threat actually happening
- maximum impact from threat actually happening (without protection measures) with respect to:
  • CII operational continuity capability,
  • direct and/or indirect economic losses

also in relation to interdependencies with other critical infrastructures;

• estimating CNI vulnerability level in relation to considered threat, which means estimating the effectiveness of prevention measures (ability to reduce expected threat frequency) and protection measures (ability to reduce threat impact). Please observe that vulnerability level is strictly correlated to the destructive potential of natural event or attack.

Under the methodological viewpoint, the analysis stage requires:
• the definition of a metric for the qualitative and/or quantitative measurement of threats impact;
• the definition of a metric to measure vulnerability level associated to the various threats;
• the establishment of a periodical process in which threat and vulnerability analyses are constantly repeated in order to take stock of changing conditions (change might be gradual or linked to the occurrence of specific risk magnifying factors such as international crises, extreme weather conditions being forecast, etc.).

Under the operational viewpoint, the analysis requires:
• the establishment and update of log journal concerning past accidents/attacks and their consequences;
• the availability of database containing standard reference threats related to the kinds of risk units to which they might apply;
the availability of database concerning rare threats which, however, might have a relevant impact on infrastructures;

- the constant updating of professional skills in the field of new technologies;

- the availability of communication channels to exchange critical information for survival with security bodies belonging to other infrastructures.

2.2.3.2.1 Threats against CII and related communication systems

Generally, threats against CII and, in particular, against related communication systems, can be defined in terms of sources, involved resources, motivation, feasibility, aim and outcome.

In our context, possible threat sources might be:

- Foreign countries
- Terrorists
- Hacker/Hacktivist
- Criminals
- Cracker
- Insider
- the Environment
- Script kiddy (involuntary sources).

For the sake of our analysis, referring to Table 3 might be useful since it describes some threats, against CII and related communication systems, with the indication of their possible accidental or intentional nature.
<table>
<thead>
<tr>
<th>Type of Threat</th>
<th>Threat</th>
<th>Accidental</th>
<th>Intentional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Fire</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Water damage</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Pollution</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Major accidents</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Weather</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Earthquakes</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Volcanoes</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Lightning strikes</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Floods</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Air conditioning system failure</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Power supply failure</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Hardware destruction</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Hardware theft</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Espionage</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Sabotage, vandalism, illegal use, fraud or physical</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>intrusion/replacement</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thermal radiation</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High intensity electromagnetic pulses</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communication interruptions</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Electronic</td>
<td>Electromagnetic interference</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Communication tapping</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>Missing/Altered originator authentication</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network data alteration</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network data extraction</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operational blockage</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Human factor</td>
<td>Internal information disclosure</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>External information disclosure</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Unavailability of relevant staff</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Errors or shortcomings on the part of relevant staff</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Document theft</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Material theft</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unauthorized system control acquisition</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unauthorized use of materials</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Terrorist actions</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Strikes/civil unrest</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intentional omissions or errors</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>ICT Infrastructures</td>
<td>Hardware damage or failure</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hardware saturation</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software error or failure</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data entry error</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inappropriate system use</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inappropriate maintenance</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unauthorized data base or system modifications</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Masking</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Denial of Service (DoS)</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use of analysis monitoring and infiltration systems</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use of malicious codes or systems (Malware)</td>
<td>*</td>
<td></td>
</tr>
</tbody>
</table>

*Tabella 3: Threat Partition*
2.2.3.2.2 Specific Vulnerabilities of CII Communication Systems

CII communication systems have become increasingly vulnerable due to a number of technical-organizational factors that have characterized choices and innovations, both on the Customer side as well as the Supplier/Provider side such as:

1. The gradual introduction in CII networks of standard architectures and protocols which were developed for Internet (TCP/IP). These architectures are also introduced in strategic control applications for geographically distributed processes (e.g. SCADA applications) which were previously characterized by proprietary protocols and strictly private networks.

2. The proliferation of CII networks implemented on “virtual private network” (VPN or IP-VPN) solutions, with «mission critical» traffic passing through multi-service public networks.

3. The need to establish interconnections between CII networks and other (internal or external) networks for operational reasons and allow distributed remote access for standard or unscheduled supervision and management activities (24/7).

4. Congestion management and security implementation problems related to networks made up of several independent sub-networks.

5. Increasingly frequent O&M outsourcing, carried out by TLC providers for their technology, has led to a proliferation in the number of authorized providers so that now there is a greater need for authorization rules and supervision.

6. Frequent network failures caused by third parties on local loops providing connectivity, e.g. underground cables. The introduction of new connections following liberalization has not entailed any remarkable change for this specific
threat, since the principle of shared link use is often resorted to in order to optimize costs. The impact coming from this kind of damage is correlated to existing redundancy, to the part effectively guaranteed by Provider (physical diversification), as well by the amount of data which is transferred through the physical link. As an example of specific threats affecting such Communication Links please refer to Table 4.

7. Human error, which might cause damage or failure.

8. The increasing dependence of public network platforms, which often support CIIs’ communication networks, upon complex software and database and, sometimes, upon the Internet.

9. More and more standard operative support systems (OSS) being used for public networks and widespread information available on these systems’ control (COTS) which are therefore accessible to a number of “potential enemies”.

10. The persistency of Host vulnerabilities requiring optimization, despite the fact that the Internet is becoming increasingly secure, by implementing security protocols which affect the higher OSI levels.

11. Critical dependence, in IP networks, upon routing and address translation services. The list of connected critical services is growing regularly including directory services and public key certificates which, in turn, generate other critical services.

13. The increasing routing capacity of network protocols which leads to an increase in related risks.

14. The inadequacy of routing algorithms which do not achieve optimum scaling, require computation power and do not have flexible policies: problems related to algorithm stability and routing changes must be solved whenever a failure on network components occurs.
2.2.3.2.3 Threat-Service Correlations

An example of threat-service correlation is reported in Table 5, where only some of the possible threats are considered in relation to the main category of services, after having made sure that other threats do not have a statistically significant impact (a typical example would be an earthquake in a non-seismic area or floods in areas distant from the sea, rivers or lakes).

Services which might become degraded in case of failure in the network infrastructure by which they are supported are listed here under macro-categories:

- **e-mail**: different email categories and, more in general, messaging systems

<table>
<thead>
<tr>
<th>Threat</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vibration</td>
<td>Train, subway and vehicle traffic, seismic activity, construction or maintenance activity in progress</td>
</tr>
<tr>
<td>Fluid penetrating through cables</td>
<td>Water and other fluids</td>
</tr>
<tr>
<td>Radiation</td>
<td>Nuclear, Narrowband electric fields, Broadband fields</td>
</tr>
<tr>
<td>Temperature</td>
<td>Fire, accidental or arson, high temperature in a confined space</td>
</tr>
<tr>
<td>Exposure to fire</td>
<td>Forest fire, fuel fire, vehicle accidents, burning gas leak</td>
</tr>
<tr>
<td>Wind and ice</td>
<td>Hurricanes, tornado, simultaneous exposure to ice and high winds</td>
</tr>
<tr>
<td>Construction activities</td>
<td>Human error, excavation activities</td>
</tr>
<tr>
<td>Corrosion</td>
<td>Industrial chemical environment, coastal environment, car and heavy truck traffic</td>
</tr>
<tr>
<td>Lightning strikes and power overload</td>
<td>Lightning, high voltage</td>
</tr>
<tr>
<td>Power supply failure for telecommunications apparatus</td>
<td>Extended power failure</td>
</tr>
</tbody>
</table>

*Table 4: Example of threats against communication links*
### Table 5: Services/Threats

<table>
<thead>
<tr>
<th>Category</th>
<th>Type of Threat</th>
<th>Management Services</th>
<th>Infrastructures</th>
<th>Critical Infrastructures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>email</td>
<td>web based</td>
<td>Enterprise IP services</td>
</tr>
<tr>
<td>Natural Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Essential Service Intermption</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Terrorist Attacks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Epidemics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacker Attacks</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Internal corporate events</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HW Failures</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>HW and SW System Maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sabotage and Other Internal Attacks</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Interdependence with Third Parties</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **X**: Service vulnerable to threat
- **Y**: Service vulnerable to threat but application (non network) countermeasures are in place
• **Web Based**: internal or external services generally based on WEB/Browser interface

• **Enterprise IP Service**: this includes a rather wide range of IP-based business applications used for management purposes. As a matter of fact, this category includes a complex group of applications (integration framework) with varying degrees of critical importance

• **Contact Center**: Infrastructural and application services which allow the Company to be contacted by its customers/users through different links. Hence this category includes CRM, IVR, CTI services as well as document-management services.

• **Wired Telephony**: a Company’s internal and external communication services

• **Mobile Telephony**: services for corporate mobile communications

• **Process Control**: local or remote equipment and system control services, for monitoring, control and accounting purposes

• **Critical Process Control**: local or remote equipment and system control services, whose appropriate and constant availability is essential for the provision of core-business services

• **Security**: generally speaking, services which are necessary to ensure infrastructure security through adequate protection systems. For example, this category includes surveillance systems, IT security applications (PKI, SSO System etc). Of course, it can be broken down further into subcategories.

### 2.2.3.3 Risk Assessment and Analysis

For this kind of assessment, collected data are processed to come up with a global risk level estimation to which the CII is exposed.

Generally speaking, the risk level related to a given threat is normally considered to be equal to the (statistically) expected damage
deriving from the threat occurrence during a given timeframe.

Using the parameters which were estimated during the threat and vulnerability analysis stage, the level of risk associated to a given threat can be expressed in relation to threat frequency, maximum impact (in its direct and indirect components due to side effects) and vulnerability level.

The introduction of countermeasures leads to a reduction in CII vulnerability levels in relation to a specific threat and, hence, to a reduction of threat frequency and impact. In the case of threats which derive from voluntary actions, the introduction of security measures can also lead to a reduced frequency in threat occurrence.

Therefore, the introduction of security measures to counter threats causes a reduction in the overall risk to which CII is exposed.

When risks which are peculiar to communication networks are being analyzed, the following activities are carried out:

- Classifying all data in order to identify the most critical information
- Analyzing critical systems which make up the network and, for each system, determining an IT intrusion risk coefficient
- Defining technological, organizational and logistical countermeasures to be implemented to reduce risk level associated to the above-mentioned critical components. Different risk-reduction strategies might be adopted, adjustable to different risk-management policies which are implemented.
Operations to be performed are:

- **STAGE 1 – Identification and Assessment of the following assets:**
  - *Data* (Information contained in IT systems)
  - *Software* (system/application)
  - *Physical Assets* (Hardware)

  Considering losses which might be incurred if such assets were discovered (loss of confidentiality) or modified (loss of integrity) or made unavailable (loss of availability).

- **STAGE 2 – Threat and Vulnerability Analysis:**
  - Identification of threats against assets (or asset groups)
  - Threat level *assessment* (high, medium, low), hence of the probability of threats happening
  - Identification of asset (or asset group) vulnerabilities
  - Vulnerability level *assessment* (high, medium, low), meaning the probability that a threat might be successfully carried out by exploiting that specific vulnerability
  - *Assessment* of overall risk level calculated in relation to assets value and estimated threat and vulnerability levels. This assessment must also include an “Image” factor which could have a huge economic impact.

- **STAGE 3 – Countermeasure Identification:**
  - *Risk prevention*: preventing risks means avoiding any specific activity which might entail risks (e.g. to prevent the risk of disclosing particularly sensitive IT data, these data can be eliminated from the system)
  - *Risk reduction*: reducing risks at an acceptable level requires the adoption of appropriate countermeasures
- *Accepting identified risk:* finally the fact that the system is anyway exposed to a risk, although it has been reduced as much as possible, has to be accepted. It has to be considered the fact that it is not possible to build a totally risk-free system, for once because it would be extremely difficult to use (due to the presence of excessively restrictive procedures) and then because it is impossible to foresee all possible attacks which can be perpetrated from the inside or the outside.

Therefore, in the end the outcome of this analysis leads to choices (Risk Management): once assets have been listed, threats and vulnerabilities have been identified, possible reasons motivating perpetrators have been analyzed, costs and benefits of possible countermeasures have been examined, countermeasures which are considered to be suitable to prevent and/or reduce risk will be chosen. Therefore, not all countermeasures that have been identified have to be implemented. They might be made looser for economic or feasibility reasons. Risk will increase but under a cost/benefit viewpoint it will be an acceptable risk. The most important message is to envisage at least one countermeasure for every attack against assets which are considered “valuable” for the system.

*Figure 5: Risk Analysis Stages*
It is worth recalling the principle by which total security does not exist. Attacks which are able to overcome any countermeasure are always a possibility, but those attacks too have a cost. To discourage them it is usually enough for them to be more costly than the benefit which might be obtained if carried out successfully.

### 2.2.3.4 Risk Management Strategy Definition

During this stage, which is closely related to risk assessment, maximum acceptable risk levels are defined and strategies to reduce risk below such levels are chosen.

Risk levels can be reduced by introducing protection measures which decrease vulnerability levels, but in some cases other factors can be used such as threat frequency.

The analysis process must lead to:

- selecting the most appropriate protection strategy and measures;
- optimizing the use of (human, economic, technological, etc.) resources allocated to security;
- documenting decisions made and communicating them to those who must implement them.

Most important in this stage is the availability of a database containing active, passive and organizational security measures in relation to the threats they are able to counter.

### 2.2.3.5 Choice Effectiveness Verification

The verification process is meant to provide for constant CII monitoring, aimed at understanding whether security measures which have been implemented are really able to reduce risk to desired levels. If this is not the case, the process will have to provide the necessary
information so that appropriate corrective actions can be introduced.

Corrective actions might concern the way in which protection measures have been implemented, threat and/or vulnerability impact level assessment criteria, calibration parameters of algorithms used to calculate risk level, etc.

Therefore, the verification process is a learning process (incident learning) which must rely on effective incident warning systems and which requires the creation of a database in which such warnings are collected, together with any information which is considered useful for a total understanding of incident causes.

As the database contains an increasing number of incidents, collected information will allow for a better statistical knowledge of relevant events and, based on a comparison between expected damage and real damage, will allow for constant monitoring of solutions adopted effectiveness with changing conditions over time.

2.2.3.6 Operation Procedure Simulation and Testing

Even if risk analysis is constantly updated and operational procedures turn out to be in line with the new data emerging from the analysis, it is nonetheless essential to establish a process which allows for the theoretical and practical simulation of accidents and attacks in order to verify the structure’s and organization’s response to such events.

This stage requires the following actions to be carried out:

* performing periodical tests to verify whether the structure is really secure;
* performing periodical accident simulations to verify structure effectiveness and related response times.

For the process to be implemented, it is essential to identify a dedicated team which is not involved in routine management and is tasked with performing periodical tests.
Once it is up and running, this team must receive the results coming from updated risk analyses, together with a “map” of business processes, so that they can prepare a document which describes in detail single impacts on core-business and areas in which improvements can be made.

2.2.3.6.1 Operation Procedure Testing

Simulation must be the starting point for reaction analyses in case of accident. Simulations must be carried out considering all possible kinds of accidents which were detected through risk analysis.

As soon as this stage is over, it is important to carry out so-called “field-tests”. Often even the best procedures and simulations fail in front of typical “unaccounted switch”. Carrying out tests can show what kind of impact on business might be generated, since the voluntary causing of an accident might produce effects which had not been foreseen during the simulation stage.

A good way to limit impacts is using dedicated testing environments: it is important to consider as an axiom that the more a testing environment differs from real life, the more testing turn out to be ineffective. In normal conditions, the idea is to perform systematic tests in testing environments in order to enhance incident learning processes, and to perform a limited number of tests in the real environment.

Analyses carried out during tests are essential, and must envisage different observation levels concerning business activities, IT services and technology infrastructures. All collected data must be fed into the risk analysis and will have to support management in identifying what actions should be implemented.

2.2.3.6.2 Accident Simulation

Accident-simulation techniques rely on results coming from risk analysis and consolidated business activity procedures.
The ideal scenario would be to develop a flexible IT tool based on a mathematical model which is able to react to changes in the above-mentioned results.

The model must envisage an appropriate counter reaction, since a change in any possible initial status might entail manifold status changes due to a cascade effect. After having developed the model, then it is possible to move on to the simulation stage: basically, whatever is caused by a change in the initial system status will be analyzed. This analytical phase is necessary to carry out targeted tests in testing environments, with the aim of minimizing implementation costs and efforts. Tests carried out in testing environments must be as similar as possible to the real environment where business activities take place.

Fundamental aspects are: the identification of (IT, technological, etc.) observation levels and the definition of metrics with which simulations will be evaluated.

Only a careful metrics definition will allow for a comparison between the results coming from different simulations and clearly identify an event’s critical level.

2.2.4 From CII Protection to Related Communication Systems Protection

It is advisable to underline that in this document the notion of Communication System is meant in its broader definition which also includes Information System which is necessary for its operation.

In this framework, in order to deal with CII’s Information System security in a meaningful way, it must stress that solution has to be sought not only for purely technological aspects, but also for organizational, training and procedural aspects.

Under the technological/organizational viewpoint, CII protection can be broken down into the following areas:

- **Physical Protection** – That is all those actions which become necessary to avoid that accidental or intentional events might affect support physical structures.
In this context, we should mention:

- Surveillance systems
- Physical protection systems
- Monitoring sensors
- Access control mechanisms

Of course, this area also includes so-called “smart” devices such as sensors and actuators:

- Disseminated sensors and actuators
- Highly automated management, command and control systems
- Smart alert detection systems
- Remotely manageable systems and apparatus.

- **Logical-structural protection** – This kind of actions consists in:
  - Architectural strengthening (HA class systems)
  - Redundancies
  - Traffic separation
  - Creation of alternative backup communication links
  - Disaster recovery systems
  - Secondary power supplies (UPS and standby units)
  - Staff training
  - Certifications.

- **Communication Protection** – seen as all those actions which are meant to ensure information flow continuity and appropriateness and, in particular:
  - Quality of Service level
  - Management of priority levels to be assigned to critical traffic for operational continuity and survival
- Information encryption
- IT security systems (firewall, anti-virus)
- Information system security management system (IDS).

The following chapter will be specifically dedicated to Information System protection in the three areas we have just described: i.e. physical, logical and communication.
3.1 INTRODUCTION

In this chapter we will analyze the “Communication Network” performance requirements associated to the aforementioned CII and the related Information System to ensure functioning of these networks. In particular, we will analyze in greater detail CII peculiar features, using communication systems based on the IP protocol family as they represent almost all implementations currently in use.

3.2 COMMUNICATION NETWORKS FOR CII STRUCTURES

3.2.1 Functional performance for sensitive communication networks for service guarantee purposes

Table 6 defines, in terms of Functional Requirements, the main performance-related aspects required from a general Communication Network supporting CII operations. The SLA (Service Level Agreement) concept is introduced as fundamental instrument to regulate the relationship between the client (CII) end TLC service providers.
<table>
<thead>
<tr>
<th>Functional Requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced priority management</td>
<td>The emergency service takes priority over all other traffic</td>
</tr>
<tr>
<td>Secure network</td>
<td>The network must be protected against unauthorized access, including encryption and user authentication techniques</td>
</tr>
<tr>
<td>Non traceability</td>
<td>Selected users can use the network, without any risk of being traced</td>
</tr>
<tr>
<td>Restorability</td>
<td>When a breakdown occurs, the service should be restored at the expected level, on the basis of priorities</td>
</tr>
<tr>
<td>International connection (*)</td>
<td>The service should guarantee access to international carriers</td>
</tr>
<tr>
<td>Interoperability</td>
<td>The service should guarantee interconnection with other selected networks</td>
</tr>
<tr>
<td>Mobility (*)</td>
<td>The communication infrastructure should be transportable, reusable or fully mobile (e.g. GSM, satellite, HF,…)</td>
</tr>
<tr>
<td>Coverage (*)</td>
<td>The service should be accessible from any primary station</td>
</tr>
<tr>
<td>Survival – Resilience</td>
<td>The service should be robust, able to guarantee continuity, despite any intentional and accidental threat</td>
</tr>
<tr>
<td>Voice</td>
<td>The service should guarantee voice transmission</td>
</tr>
<tr>
<td>Broad Band (*)</td>
<td>The service should guarantee video, image, multimedia transmission</td>
</tr>
<tr>
<td>Band scalability</td>
<td>There should be the possibility to change bandwidth within a pre-established range without replacing the HW</td>
</tr>
<tr>
<td>Growth capacity</td>
<td>The service should be able to multiply the network capacity</td>
</tr>
<tr>
<td>Availability</td>
<td>The service should comply with the design requirements and should be usable when it is needed</td>
</tr>
</tbody>
</table>

Table 6: CNI network requirements. The items marked with (*) are functional requirements to meet where necessary and required.
3.2.2 Solutions for communication networks

3.2.2.1 Current networks for CII infrastructures

We can generally represent currently used Critical Infrastructure Communication Networks on the basis of the following common features:

- rarely owned by the critical infrastructure, they generally rely on market operators
- the purchased services vary enormously, ranging from intranet to VPN solutions, up to totally open world networks such as the Internet
- some of the aforementioned implementations manage Information Security through the following solutions:
  - Firewall
  - Antivirus
  - Encryption (end-to-end, bulk encryption)
  - Authentication (PKI)
- Given their global coverage, Wireless Networks that are generally highly critical in terms of connectivity and information protection, are widely used
- QoS (Quality of Service) guarantee is often poor and is identified with the capacity to normally provide services without performance details in terms of:
  - absence of “single point of failure”
  - sufficient or defined connectivity
  - guarantee of “graceful degradation”
- Differentiated data management capacity is generally lacking in terms of “Normal, Secure and Strategic Data”
- Also the application of the concept of “Isolated Network”, that is a network that does not require connection to other networks that might be a source of information attacks, is missing.
Furthermore, it seems that Network Federations are not used/provided, nor are networks using different transmission media (with the exception of “down hill” radio link applications as access to EARTH networks).

Some Critical Infrastructures have lately started to take seriously into consideration Communication Security-related aspects.

A typical example is Terna that recently decided to go back to “private network” solution development, thanks to technological evolution and to the features of high-voltage electrical infrastructures.

Specifically, Terna is developing its own ATM architecture for control data transmission purposes (for remote management and monitoring of the National Power Transmission Network). The new infrastructure uses digital signals transmitted through high-voltage power lines as transmission media. This way the infrastructure is isolated and completely autonomously managed and therefore, it is able to offer high quality and security levels. The project started as integration and enhancement of the operating networking platform based on market resources; however, it offers interesting in-sourcing prospects.

3.2.2.2 Network (and their interaction) model to achieve the requested performances

3.2.2.2.1 Preamble

This section presents some solutions concerning the implementation of security requirements in Communication Networks; these solutions and indications are in line with the Good Practice and consequently with the expertise acquired at the national and international level and with state of the art trends.

The solutions described below are developed through the following process:

- from basic communication network security requirements, the basic services and the methodological approach to characterize secure networks are defined
- communication network features are then identified accord-
ing to the security level to be achieved by defining global characteristics (mainly QoS, connectivity and information security) at the level of «stand alone» network

* The various details concerning the following aspects are developed:

- the “connectivity” of a single network
- the possibility to increase connectivity through the “network federation”
- information security-related aspects in terms of accesses (Network Port) and application (Middleware)
- Data Centers and Data Usage Structures
- power supply related issues

* Finally, a short description of possible Emergency Networks.

Clearly all this must always be supported by a rigorous analysis of risks and consequences, carried out by means of the methodologies described in the previous chapter.

3.2.2.2 Basic network security requirements

Herewith the solutions that can be applied to successfully handle security issues in the field of information networks will be provided.

Given the current context, it is difficult to provide precise technical indications to follow for maximum security applications; nevertheless, it is possible to describe the minimum basic requirements for Communication Network security.

On the basis of what was already defined in Chapter 2, the fundamental network security requirements are listed below (Fig. 6):

* Availability: the capacity to access critical data for the infra-
structure survival anytime even if the network is operating under extreme conditions

- *Data source authentication*: the capacity to identify a user that is appropriate to the specific information and service type

- *Access control*: ensures that only authorized users can access network resources

- *Data confidentiality*: ensures that only authorized users can access protected data.

- *Data integrity*: ensures that data is not altered by unauthorized users or non guaranteed software or hardware

- *Non rejection*: it provides indisputable evidence of successful data delivery or reception over the network.

Furthermore, in the case of CII networks, it is necessary to
guarantee that authentication systems can be shared according to the specific needs using the following:

- a coordinated system for encryption key generation, distribution and management based on PKI or proprietary architectures, but in any case hierarchical and distributed
- access control systems should take into account the need for a distributed certificate validation system to be able to serve hundreds of thousands of users, ensuring reliability, high performance, security, and minimum installation costs.

In order to avoid interferences from foreign networks to both public and private CII networks, two possible alternative solutions can be applied:

- complete separation of CII networks from other networks
- application of special security systems to connect external networks to CNI networks.

The complete separation of CII networks from other networks ensures a high level of security against intrusions or malfunctions from outside. The US “Govnet” network is an example of an independent administrative network that was designed as a private voice and data network based on the Internet Protocol (IP) but without interconnection with commercial and public networks. The same applies to the Italian FF.AA networks (for example MARINTRANET and DIFENET) that meet the requirement of functioning with no risk of external intrusions or interferences, in order to guarantee confidential or sensitive data security.

However, especially under normal condition, it is virtually impossible to separate CII networks from the external ones because they have the need or the convenience to interconnect to other networks to exchange essential data and for commercial or financial purposes. Hence the importance to ensure maximum network interconnection security under these conditions, using suitable protection policies and technical solutions that guarantee full access and data exchange security both at the network port and user level.

The necessary steps in the methodological approach, which...
can be applied when designing a new secure network as well as when secure an existing network, are the following:

- characterizing the network or service type
- performing an accurate risk analysis
- verifying the network architecture’s distinctive elements to make it comply with CII security standards
- defining the network gateway to securely access other CII infrastructures’ networks and external networks
- equipping the system, also at the middleware level, with appropriate security measures applications and procedures.

The application of the following five principles ensures the implementation of a secure network with the appropriate cost-efficiency ratio:

- risk and requirement auditing
- establishment of a central network security team
- enforcement of the most appropriate security measures and of the related security inspections
- awareness distribution of the risks connected to non application of security regulation
- control and auditing of measure and security control efficiency.

### 3.2.2.2.3 Characterization of network types

From the viewpoint of those who propose, design and implement a network and the services based on such network, it is essential to assign to a limited number of categories the many different realities of CII networks.

The various cases into which the networks should be subdivided should meet the following basic criteria:

- area coverage
network bordering

availability of communication structures

From the area’s coverage point of view, a CII network can have a local coverage or be extended at the national level. In this latter case there may be a widespread location distribution, with locations of very different importance, or the distribution may be limited to a few locations of comparable importance.

Table 7 shows some examples of CII, referred to the Italian scenario, to explain this concept.

<table>
<thead>
<tr>
<th>Local area’s coverage</th>
<th>Extended national area’s coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited location distribution</td>
<td>- The naval bases or arsenal of the Navy&lt;br&gt;- Data Processing Centers of Inter-banking Services</td>
</tr>
<tr>
<td>- A Local Health Care Unit&lt;br&gt;- Transport system establishment (e.g. underground railway)&lt;br&gt;- A port docks, goods handling and storage areas, customs</td>
<td></td>
</tr>
<tr>
<td>Widespread location distribution</td>
<td>- The Carabinieri stations&lt;br&gt;- Telecom Italian switching stations&lt;br&gt;- Railway stations&lt;br&gt;- ENEL power stations</td>
</tr>
<tr>
<td>- A Bank present in a Province’s territory&lt;br&gt;- A local Utility’s plants</td>
<td></td>
</tr>
</tbody>
</table>

*The impact of this on the network is immediately clear.

- The local coverage makes economically competitive the implementation of networks using private transmission media, as in the case of a wireless network or of a fiber optic network, covering a port or a hospital. Few companies (in Italy, Ferrovie, RAI, Department of Defence, the various Telecom companies) can afford building up (or they already have) national networks using private transmission media.
The widespread distribution of locations brings about important problems in the implementation of secure networks; indeed network vulnerability increases as the number of access points grows up. Due to economic and geographical reasons, this type of networks tends to be implemented at several levels, thus introducing concentration points. The presence of concentration points increases network vulnerability. A widespread location distribution makes it also necessary to adopt access protection systems at limited costs, to cover access networks that are very complex.

Table 7 can therefore be “re-read” in terms of architectural characteristics, as shown in Table 8.

<table>
<thead>
<tr>
<th>Limited location distribution</th>
<th>Local area’s coverage</th>
<th>Extended national area’s coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN or MAN networks</td>
<td>- Access Network often absent</td>
<td></td>
</tr>
<tr>
<td>Limited location distribution</td>
<td>- Low or medium cost private transmission media</td>
<td></td>
</tr>
<tr>
<td>- WAN networks connecting a limited number of “islands”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Generally non complex access networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- High cost private transmission media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Widespread location distribution</td>
<td>- Networks that already present WAN characteristics on a small scale</td>
<td></td>
</tr>
<tr>
<td>- Complex access networks with concentration points</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Medium to high cost (related to the total number of locations) private transmission media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Widespread location distribution</td>
<td>- WAN networks, often structured with multiple levels</td>
<td></td>
</tr>
<tr>
<td>- Very complex access networks with concentration points</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- High or often unaffordable cost (related to the total number of locations) private transmission media</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 8: Architectural Characteristics of CII Networks

A second criterion is network bordering. A confined network is closed and separated from the “external world”, that is from any other network, public or belonging to other organizations. An intranet network is a good example of confined network.
Some organizations do not want or cannot use a confined network model: let us think, for example, to the opportunity offered to citizens to receive certificates from the Municipality of residence through e-government procedures.

A network can be confined at both physical and logical level. Maximum security networks are clearly both physically and logically confined. A network that is confined neither physically nor logically is called “open” network. Internet is a good example of an open network. Generally, being physically confined for a network, it also implies that it is logically confined. However, the vice versa is not necessarily true; as a matter of fact many logically confined networks in reality rely on physical links supplied and managed by external organizations (Service Provider).

In a confined network all users are known or at least belong to known categories. This simplifies access management unlike a non-confined network where even anonymous users provided with sufficient credentials can be accepted. These credentials are often granted by an “accredited third party” (or Certification Authority).

The third criterion is the availability of communication structures at a specific organization, that is sites or infrastructures that support or may support a telecommunications network.

Depending from its own local coverage, an organization may be provided with optically visible sites that can support the creation of a telecommunication network, with a given transmission media, at a given price. When this is not the case, and especially when there is an extended local coverage and a widespread location distribution, the organization can equip itself with a secure network by relying on third party’s transmission media. The most convenient solution depends on the auditing carried out in the network design and, in particular, on the reliability and availability of the physical network.

A secure network design should start from the definition of two fundamental elements, namely:

* the definition of security level the Customer requires
* the definition of the network operating requirements.
The definition of security level the organization should cover involves several aspects, such as:

- the definition of the information security level(s)
- the definition of the requested QoS parameters
- the definition of the requested data integrity(s)
- the definition of the threat against which the network should be fully operating or partially operating, only managing “essential” data
- the definition of the network portion that should operate under maximum security, the portion under medium security and the portion under low security (open world)
- any other aspect related to the definition of the requested security

The definition of the network operating requirements shall include, inter alia, the following aspects:

- number of users
- any individual user or individual LAN type
- peak traffic
- assigned priorities
- security levels
- importance
- user locations
  
  requested connectivity and possible use of a range of transmission media (cable, radio link, satellite, etc.)

3.2.2.2.4 Periodic maintenance of production system

The defined Protection System is affected by logistic and technological changes and it is therefore necessary to guarantee that such changes are reflected in the system.
Below there is a list (incomplete) of the events for which Protection System updating is required:

- changes in the national legislation
- organizational changes
- changes in the security objectives
- identification on new types of threats
- identification on new types of vulnerability
- technology evolution
- changes in the scope of intervention

These changes call for a revision of the entire aforementioned Risk Analysis cycle, from its requirements and basic presuppositions. The prompt adjustment of the Protection System and of the related documentation is important from the point of views of the efficacy of the protection level provided; it becomes indispensable in case a Protection System Certification is required.

### 3.2.2.2.4.1 Security auditing and certification

The term “security certification” means the auditing and certificate, provided by independent, qualified and officially recognized third parties, of a system, product, process or service compliance with the security requirements provided by a standard or a reference regulation.

The ICT security auditing and certification process should have the following characteristics:

- **Repeatability**: given the same security objectives and requirements initially imposed, the auditing process should lead to the same final outcome if carried out once again by the same Auditing Body.

- **Reproducibility**: given the same security objectives and requirements initially imposed, the auditing process should lead to the same final outcome if carried out once again by another Auditing Body.
• Impartiality: the auditing and certification process should not be influenced by external factors

• Objectivity: the outcome of the security auditing should be based on fact as immune as possible from subjective opinions or experiences.

The fundamental aspects that in the real world make useful and efficient a security auditing and certification process are, therefore, the proven efficacy of reference standards and the real third party nature of certification and auditing bodies towards end users, system developers, process or product and certification process financing parties.

In the specific case of security certification, a first aspect is considered as met whenever standards tested over time by several subjects are applied and implementation modalities are identified that, on the one hand, turn out to be efficient to improve ICT security and, on the other hand, allow an effective integration of security measures with the production processes of the Organizations that use them.

As to the second aspect, a valuable guarantee as to the third party nature of the certification process can be represented by the fact that at least certification Bodies, if not the security auditing Bodies, are officially entrusted with the task by the State where they operate and/or are recognized by independent international organizations.

In the specific case of critical infrastructures, the national technical committee on information technology and telecommunication security in public administrations shall recommend that at least ICT systems/products that manage information and applications requiring a high level security are submitted to certification according to the Common Criteria or ITSEC criteria. This indication is in line with what is provided by DPCM “Approval of the National Scheme for certification and security auditing in the Information Technology field, as laid down under art.10 paragraph 1 of Legislative Decree 10/2002”. For example, the document “National Security of Telecommunications and Information Systems” edited by the “National Security Telecommunications and Information Systems Security Committee (NSTISSC) suggests using security certification for systems han-
dling information that, although it is not classified for national security purposes, may be considered as critical or essential for the exercise of the primary functions of the Administration, as well as for the systems on which the operability and/or the maintenance of critical infrastructures depend.

Furthermore, the document “The National Strategy to Secure Cyberspace” – US government document – February 2003, states that the US government intends to evaluate, form the financial feasibility point of view, the extension of the certification obligation to ICT systems/products used by all federal agencies, also when they do not handle classified information. The US government also provides that, should that extension be implemented, it would very positively affect the ICT product market with the benefits being enjoyed also outside the government context. Two main certification types for ICT security that are today in use were standardized by ISO/IEC, although for one of them the process cannot be considered complete. More precisely, in 1999 ISO/IEC adopted a complete series of criteria known as “Common Criteria”, allowing the evaluation and certification of ICT product and system security. This adoption was formalized through the issuing of the ISO/IEC IS 15408 standard.

As to the second type of certification, in the year 2000 ISO adopted only the first part of the BS7799 standard developed in Great Britain. In the ISO/IEC version it is called IS 17799-1. The second part of the standard, containing more precise indications concerning certification, it is now only available as British Standard Institution standard.

The ISO/IEC IS 15408 (Common Criteria) standard and the ISO/IEC IS 17799-1 and BS7799-2 pair of standards are intended to certify two well distinct things: in the case of the Common Criteria (CC), the object of certification is an ITC system or product; in the case of the BS7799 standard what is certified is the process used by an

---

5 An ITC system, according to the terminology used in the CCs, is an IT installation used for well defined purposes in a completely defined operating environment. An ITC product, instead, is a hardware device or a software package designed for usage and installation in a wide range of systems.
organization, be it a private company or a public structure, to internally manage ICT security. In the standard, this process is indicated with the acronym ISMS which stands for “Information Security Management System». The BS7799 certification can be considered a corporate certification, like the well known ISO 9000 certification, but specialized in the field of ICT security.

Specifying the certification object is appropriate since some of the characteristics in the British BS7799-2 standard might beget confusion and make people believe that the related certification may make the Common Criteria certification almost superfluous. As a matter of fact, amongst the requirements an organization must meet to be BS7799 certified, some of them represent functional requirements of the organization’s ICT systems/products.

However, for the BS7799 certification purposes, it is sufficient to verify that the aforementioned functional requirements are selected on the basis of a correct risk analysis and management and, through the use of sampling, verify that the corresponding security functions are present on ICT systems whenever necessary. For the Common Criteria certification of one of the organization’s ICT system/product, it would be necessary, instead, to verify that the aforementioned functionalities do not have implementation-related faults and are able to resist, up to a fixed severity threshold, to a set of threats specified in a well defined environment.
3.2.2.2.4.1.1 The Common Criteria

The rational at the basis of the Common Criteria (CC) was drawn from the previous European ITSEC\(^6\) criteria (Information Technology Security Evaluation Criteria) that had first introduced it. According to this rational, it does not make sense verifying if a system/product is secure if the following are not specified:

- “secure” to do what (security objectives)
- “secure” in which context (security environment)
- “secure” following which auditing (guarantee requirements).

According to the CC, a security objective is defined as the intention to fight a threat or to abide to existing security laws, regulations or policies. Objectives are attained through the adoption of security measures, both technical (security functions) and non technical (physical, procedural and concerning the staff).

The security environment is described in terms of:

- assumed system/product use (applications, users, processed information and other assets, specifying the related value)
- environment (non technical security measures, connection to other ICT systems)
- threats to face, specifying the attacker’s characteristics (knowledge, available resources and motivation), attack methods (mentioning, amongst other things, the exploitation of possible known ICT system/product vulnerabilities), assets involved
- security policies of the Organization.

\(^6\) In this context, we believe it is not advisable to delve into the ITSEC standard details, limiting to the description of the Common Criteria only. This choice is justified by the fact that, despite it is still possible also in Italy, to certify ICT security by applying ITSEC criteria, the European Community advises the use of the Common Criteria (see EU Counsel resolution of January 28, 2002 (2002/C 43/02).
The envisage auditing during the evaluation process aim at ascertaining that the system/product, its developer and the inspector meet appropriate guarantee-related requirements that become stricter and stricter as the auditing level increases. The CC define a 7 level auditing scale (EAL1, EAL2, …, EAL7) or guarantee level, specifying for each level a specific set of guarantee requirements.

The inspections performed on the basis of the guarantee requirements for the auditing level considered, aim at guaranteeing the following:

- suitable security functions to achieve system/product security objectives
- lack of errors in the process that from the initial security specifications (environment and security objectives) leads to practical security function implementation (technical specification interpretation errors, programming errors, etc.)
- suitable security procedures provided for delivering and installing the system/product (to avoid that the system/product delivered to end users might be, even slightly, different from the one submitted to auditing/certification), clear user and administration manuals (the latter might in fact lead users into behaviors that might introduce vulnerability in the usage of product/system provided with security functions that are fully appropriate and implemented without faults), the support the developer will provide to those who will use the system or product to make up for possible vulnerabilities emerged after auditing.
- Guarantee of the absence of faults in the security function implementation process is obtained not only by directly looking for the errors themselves (analyzing the documentation submitted by the applicant and by submitting the system/product to functional tests and attacks), but also by verifying that in the implementation process the use of tools, methodologies and procedures aimed at reducing the probability of errors was envisaged.

As the auditing level increases:
• more detailed implementation specifications are required (for example high level design, low level design, source code)

• the severity level in the description of specifications increases (informal, semiformal, formal description).

Fig. 7 shows, for each assessment level, the required specification description severity level (yellow area) and the main inspection performed during auditing (green area).

The inspection severity is not only identified by the auditing level, but also by another parameter. As a matter of fact, for the functions that must be implemented by means of probabilistic or permutation mechanisms (password, hashing functions, etc.), the CCs require (starting from EAL2) that a minimum robustness level be specified (SOF - Strength Of Functionality) on a three value scale (basic, medium, high).
The system/product security functions are described on the bases of the requirements they should meet. These requirements, called *functional requirements*, like the aforementioned *warranty requirements*, must be described (with a few exceptions that should be anyway justified) using a component catalogue included in the CCs.

More precisely, the functional component catalogue is part 2 of the CCs, whilst the *guarantee* component catalogue represents part 3.

The catalogues are organized at various hierarchical levels so as to include homogeneous components. For example, as to functional components, the highest hierarchical level provides for a group of eleven classes: *Audit, Communication, Cryptographic Support, User Data Protection, Identification and Authentication, Security management, Privacy, Protection of the TOE Security Function, Resource Utilization, TOE Access, Trusted Path/Channels* (the TOE acronym is found in some functional class names and indicates the ICT system/product to assess).

Amongst the various documents that the applicant must/can submit to the inspectors, along with the ICT system/product to assess, it is worth mentioning two of them. The first document, called *Security Target*, is mandatory and is the main auditing document. The *Security Target* should describe the security environment, security objectives, functional and *warranty* requirements (and thus the auditing level), the minimum security function robustness and an initial high level description of security functions. This last section, instead, is not included in the second document, the *Protection Profile*, whose remaining structure is similar to the *Security Target* document. The *Protection Profile* can optionally be developed with reference to a whole class of products (for which the implementation of the security functions is free provided that it meets the functional requirements) rather than to a specific ICT system/product (as in the case, instead, of the *Security Target*). The *Protection Profile* can be registered and also assessed to verify internal consistency.

The main advantages offered by an auditing and certification in compliance with the CCs are the following:

- the auditing, performed by a third party having specialist knowledge, that the security functionalities of the ICT sys-
tem/product along with the requested non technical counter measures, are suitable to meet the security objectives

- performance of preventive actions against ICT security accidents
- higher guarantees offered by the CCs compare to other preventive tools
- availability of rich catalogues concerning ICT security functions and the guarantee requirements that can be adopted
- the possibility to describe in a standard manner the security requirements for ICT systems and products.

3.2.2.4.1.2 ISO/IEC IS 17799-1 and BS7799-2 standards

The history of BS7799-type standards can be summarized as follows:

- 1999: the BSI publishes a new version of the two parts of the standard, identified as BS7799-1 and BS7799-2
- 2000: part 1 of the BS7799 standard becomes the international ISO/IEC 17799-1 standard
- 2002: a new version of part 2, the standard currently used to issue certifications, is published

The main purpose of the BS7799 standards was to establish a universally recognized and accepted standard to certify an organization’s capacity to protect its own information assets and to maintain such capacity over time. They also represent a series of best practices

---

89
in the field of information security and offer a methodological reference to manage corporate information assets security.

Each organization should protect the information it handles by correctly identifying and managing an Information Security Management System (ISMS) comprising logical, physical and organizational components. The methodology to approach the problem suggested by BS7799 standards and known with the acronym PDCA (Plan Do Check Act) provides for the execution of four steps:

- **Plan:** defining security policies, objectives, processes and procedures relevant to manage and minimize risk and improve information security so as to achieve results in accordance with the policies and the objectives of the entire organization
- **Do:** implementing and enforcing security policies, countermeasures, processes and procedures
- **Check:** assessing and, where possible, measuring process performance (with respect to security policies), objectives and practical experiences and the results are reported to the management for revision purposes
- **Act:** adopting prevention and corrective measures, based on the Management Review outcome, in order to provide continuous improvements to the ISMS.

*Fig. 8* extracted from BS7799-2, summarizes the fundamental steps of the PDCA methodology.
A fundamental aspect in the correct application of the BS7799 standard is the performance of a correct risk analysis activity. This activity’s fundamental bases are described in the ISO/IEC 13335 standard «Guidelines for the management of IT security”, one should refer to for a useful in-depth study.

Finally BS7799-2 describes in detail the security controls that must be performed, on the basis of the risk analysis carried out, by the Organization in order to verify whether the adopted ISMS was properly identified by correctly applying the approach provided for by the standard.

Security checks are divided according to the following areas:

* **Security policies**: correct identification and management of security policies over time

* **Security organization**: corporate organization and responsibilities in the field of ICT security, regulating third party access to corporate information systems and outsourcing contracts

* **Control and classification of assets to protect**: classification of corporate assets entrusted with well-defined subjects

* **Personnel security**: security behaviors for corporate assets users,
also including training on the correct use and behaviors in case of IT accidents.

- **Environmental and physical security**: physical security in working environments and of hardware and software tools

- **Communications management**: inter-corporate communication management, management of network-related aspects, protection against malicious software and failure management

- **Access control**: information access, network access, user identification and authentication authorizations

- **System maintenance and development**: use of encryption, aspects related to information integrity preservation and rules for updating and managing hardware and software systems

- **“Business continuity” management**: improving and ensuring continuity of critical functionalities

- **Adjustment to regulations in force**: ensuring compliance with regulations in force and with corporate security policies, on the part of both the organization and users

### 3.2.2.2.4.2 Security certification in Italy according to the Common Criteria (and ITSEC)

ICT system/product security auditing and certifications in Italy have been carried out since 1995 and only in the national security field.

More specifically, until spring 2002 it was mandatory to submit all ICT systems/products used in the military field to process classified information on internal and external security to certification according to the ITSEC European criteria.

Through DPCM of April 11, 2002, publish on the Official Gazette n. 131 of June 6, 2002, the certification became mandatory also for ICT systems/products handling classified information outside the military context and the possibility was envisaged to use CCs as an alternative to ITSEC criteria. The structure used for the aforemen-
tioned auditing and certifications includes a certification body, whose functions are performed by the National Security Authority – Security Central Office (ANUSUCS), and by a number of Auditing Centers (Ce.Va.).

Currently there are five accredited Ce.Va.s, two of which are part of the Public Administration, namely the centre managed by the Superior Communication and Information Technology Institute of the Department of Communications and the centre belonging to the Defense department, reporting to the Defense General Staff, Information and Security Unit, based in S. Piero a Grado (PISA)\(^7\).

To manage security auditing and certification in the commercial sector according to the ITSEC and CC standards, the DPCM of October 30, 2003 (Official Gazette n.98 of April 27, 2004) established the National Scheme for certification and security auditing for information technology systems and products. The National Scheme defines the necessary national procedures and rules in order to assess and certify ICT systems and products, in compliance with the European ITSEC criteria and the related application ITSEM methodology or with the international ISO/IEC IS-15408 (Common Criteria) standards.

Within the auditing and certification National Scheme the IT security certification Body was established (O.C.S.I.). The Superior Communication and Information Technology Institute is the IT security certification Body in the information technology field\(^8\).

The main reasons that led to the establishment of the National Scheme in the commercial sector stem from the following considerations:

- in today’s society, information is an essential goods and it is therefore necessary to guarantee its integrity, availability and

---

\(^7\) For sake of completeness also the other CE.V As are here indicated: Consorzio RES, INFORSUD, IMQ.

\(^8\) Also under art. 10 of legislative decree of January 23, 2002, n. 10 and art. 3, paragraph 4 of directive 1999/93/EC.
confidentiality by means of security measures forming integral part of an information system

- producers have been offering for a long time systems and products equipped with security functions, about which they declare characteristics and performance in order to help users choose solutions that best meet their needs

- in many highly critical applications the aforementioned indications might be insufficient, making it necessary to evaluate and certify them for security purposes by independent and qualified third parties on the basis of standards recognized at national as well as international level

- guarantees in terms of adequacy, quality and efficacy of security devices an information system is provided with may only be given by independent and impartial certification and auditing bodies

- the need to provide, at the European community and international level, cooperation between Certification Bodies and the mutual recognition of security auditing certificates in the information technology sector.

In the commercial Scheme, the OCSI carries out the following main tasks:

- defines technical certification rules on the basis of national, EU and international reference regulations and directives

- manages international relations with similar foreign bodies in order to favour mutual recognition of the respective Schemes and issued Certifications

- coordinates national Scheme-related activities in line with auditing criteria and methods

- defines Guidelines for product auditing, security targets, protection and system profiles to ensure the functioning of the Scheme

- manages accreditation, discontinuation and accreditation revocation of security auditing laboratories (LVS Laboratori di val-
utazione della sicurezza)

- verifies that independence, impartiality, reliability, technical competence and operative capacity are kept by accredited LVSs
- approves of Auditing Plans
- approves of Final Auditing Reports
- issues Certification Reports on the basis of the assessments performed by LVSs
- manages issuing and revocation of Certificates
- manages preparation, keeping and updating of the list of accredited LVSs
- manages training, qualification and coaching of Certifiers, Certification Body staff as well as Auditors, LVS staff and Assistants, to carry out auditing activities
- manages preparation, keeping and updating of the list of Certifiers, Auditors and Assistants

The auditing and certification process according to the national Scheme may be depicted as in Fig. 9.

After accrediting LVS, OCSI checks and controls the whole security auditing process carried out by the LVS itself, by guaranteeing the correct application of the National Scheme rules. The Certificate is then issued by the Certification Body.
3.2.2.2.4.2.1 Accreditation for voluntary certification according to the BS 7799-2:2002 standard

The certification process on the basis of voluntary standards, such as ISO 9001, ISO 14001, BS 7799-2 standards and the OHSAS 18001 Technical Specification, as included in the UNI INAIL Guideline, is carried out on the basis of the auditing activities carried out by the Certification Bodies operating under Accreditation. In our Country, the recognized Body that carries out Accreditation activities is SIN-CERT. However, Certifications granted under Accreditation issued by foreign bodies, signatories of the so-called MLA – Multilateral Agreement – recognized within the European Union by the EA (European Cooperation for Accreditation) and at the international level by IAF (International Accreditation Forum) are also valid. Moreover, there is an attempt to reduce through them the international trade barriers.

This mutual recognition guarantees respect of precise behavioral rules on the part of Certification Bodies that, on a voluntary basis, undergo thorough auditing carried out by their respective “Authorities” and by the Accreditation Bodies themselves, which in turn undergo rigorous inspection as provided for the aforementioned
What are therefore the basic principles regulating the accreditation of a Certification Body? First of all, the skills of the human resources responsible for the audit of the various client Organizations. Therefore a non uneven behavior towards the Organizations themselves, if belonging to different interest groups, but significantly, also the absence of any conflict of interests between the certifying body and the certified organizations. The Accreditation Body, like the Certification Bodies, should demonstrate that they are strongly representative of the various parties involved in the certification process, namely customers, consumers, manufacturers and Public Authorities responsible for market control and regulation.

Accreditation is therefore a process that provides a guarantee to the market, through auditing and subsequent surveillance, so that the certificates issued by the accredited bodies can be trusted.

Unfortunately, it often happens that in the national market also non legitimized subjects operate, thus creating confusion as to the application of rules and issuing pseudo-certifications, that cannot be of any value in negotiations with the Public Administration. These pseudo-certifications are self-referenced and, as such, cannot have the same recognized value in the national and international market as the Certifications issued under Accreditation by EA and IAF recognized Bodies.

For BS 7799-2-based certifications, SINCERT is issuing specific Technical Regulations. This documents includes additional rules for Certification Bodies (it does not apply to Organizations being certified) aimed at defining a framework of as much as possible homogeneous behaviors, with the goal of identifying characteristics of the Auditors and of the auditing rules that can guarantee a high added value not only to the Organizations that apply for Certification, but also to the market. As a matter of fact, on the basis of such recognition, the market may give certified Organizations as a whole a level of trust that can and must be guaranteed in the best possible way.

The general certification scheme according to the BS7799-2 standard is shown in Fig. 10, and differs from the one previously shown and related to the CCs in that the certificate is issued by Certification
Bodies (that may be similar to the LVSs in the CC scheme) rather then by SINCERT (that may be similar to OCSI in the CC Scheme).

Fig. 10: BS7799-2-based certification scheme

3.2.2.2.5 Network architectures supporting critical infrastructure

3.2.2.2.5.1 Secure network types

Good Practice “recommends” that issues connected to Communication Network supporting Critical Infrastructure are dealt with three different network types, namely:

- **Maximum Security Networks** to work with *strategic (critical)* data
- **Secure Networks** to work with *secure data*
- **Robust Networks** to work with *common data*

The following paragraphs describe the recommended characteristics for Communication Networks that should operate with the aforementioned data types.
3.2.2.5.1.1 Maximum Security Networks

Maximum Security Networks represent a highly reliable solution to the problems related to handling strategic and critical data whose presence, transmission and integrity must in fact be “always” granted, also under unusual conditions such as natural disasters or terrorist attacks.

Some high level typical recommendations for this type of network may be summarized as follows.

A Maximum Security Network must:

- be “isolated”\(^5\), that is separated from other non maximum security networks operating on secure or common data (open world)
  - be highly redundant (in its HW and SW components)
  - have high K connectivity (cf. par. 3.2.2.5.2)
  - be differentiated (see Fig. 11) in its typical components:
    - Redundant access network: typically mixed technique (fiber optic and/or
    - “downhill” radio link and/or wireless with differentiated redundant links at the physical level)
    - High connectivity wired backbone network, typically implemented with optic fiber links
    - radio link network to increase connectivity and, partly, the network global capacity
    - satellite network to increase connectivity
    - other transmission media, such as Conveyed Waves
  - guarantee high service levels for classes of users and priority management
  - guarantee high data integrity also when transmitting data

\(^5\) The term “isolated” refers to a Network that does not have any physical connection with users who do not belong to the network or with lower security level networks (for example, Internet).
through the different network components (for example fiber optic plus satellite)

- be sized according to the traffic it will handle (taking into account the different capacity of fiber, radio link and satellite media and, consequently, be consistently characterized in terms of user classes and priorities)

- be confined to the organization that uses, operates and maintains it, excluding, in principle, resort to outsourcing

- support appropriate encryption functionalities to guarantee protection of information in relation to processed data classification; these functionalities must be made available at each individual component’s access and transit level.

The main detailed characteristics of an example of Maximum Security Network are listed in Table 9.
<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Reference Values or Terms</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity</td>
<td>$k &gt; 2$ for access, $k &gt; 3$ for backbone</td>
<td>Implemented using differentiated physical paths (priority criterion) and/or transmission media of different nature (secondary criterion)</td>
</tr>
<tr>
<td>Availability</td>
<td>$&gt; 99.999%$ node-to-node (for each node pair) for the backbone; $&gt; 99.99%$ end-to-end (for each end-point pair)</td>
<td>Calculated on the basis of MTBF, MTTR and connectivity under normal operating conditions</td>
</tr>
<tr>
<td>Operating non-availability</td>
<td>0.1 hr</td>
<td>over one year period</td>
</tr>
<tr>
<td>Traffic-based sizing</td>
<td>Project yield performance equal to 80% on the estimated traffic peak</td>
<td>Maximum estimated traffic flow requires 80% of resources in terms of bandwidth use; the remaining 20% of resources remain available to take up other possible overloads</td>
</tr>
<tr>
<td>QoS level differentiation</td>
<td>Supported</td>
<td>By connection</td>
</tr>
<tr>
<td>Priority and pre-emption</td>
<td>Supported</td>
<td>Priority definable at multiple levels (MLPP)</td>
</tr>
<tr>
<td>Information security level and transmission resource routing</td>
<td>Supported</td>
<td>Automatically adapted on the basis of connection. Derived from the military industry</td>
</tr>
<tr>
<td>Integrity</td>
<td>Guaranteed</td>
<td>Critical data transmission through different network components</td>
</tr>
<tr>
<td>Graceful degradation</td>
<td>90% service exploitation guaranteed with 80% network functioning; 80% guaranteed service with up to 50% network functioning; no guarantee other than best possible effort for essential services and for services beyond 50% network degradation (e.g. NATO MINIMIZE, situation where the network only routes the traffic from a specific priority level and stops lower priority traffic)</td>
<td>The functioning rate is generally measured in terms of residual/nominal bandwidth over the sum of all backbone network connections. In case one switching node is out of service, all links connected to that node are considered to be out of service. The degradation percentage is the value that makes up 100% of the functioning rate.</td>
</tr>
</tbody>
</table>

Table 9: main characteristics of a Maximum Security Network
<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Reference Values or Terms</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible multi-protocol traffic (ATM, IP, MPLS, others)</td>
<td>supported</td>
<td>Considered essential in case of highly probable cyber attacks</td>
</tr>
<tr>
<td>Federation with other networks with the same security level</td>
<td>Accepted</td>
<td>It must be a priori foreseen and planned</td>
</tr>
<tr>
<td>Gateways to Internet and other networks with different security levels</td>
<td>Absent</td>
<td>No derogation admitted</td>
</tr>
<tr>
<td>Secure radio link or wireless access component</td>
<td>Generally present</td>
<td>Strongly recommended, eventually as wired link backup solution</td>
</tr>
<tr>
<td>Radio link transit component</td>
<td>Generally present</td>
<td>Strongly recommended</td>
</tr>
<tr>
<td>Satellite access component</td>
<td>Generally present</td>
<td>Strongly recommended</td>
</tr>
<tr>
<td>Satellite transit component</td>
<td>Generally present</td>
<td>Strongly recommended</td>
</tr>
<tr>
<td>Deployable component (deployable/transportable over the territory)</td>
<td>Generally present</td>
<td>Mandatory in the case of an Organization that should support provision of public services in case of disasters. It can include a deployable satellite access component.</td>
</tr>
<tr>
<td>Transit data encryption</td>
<td>Present</td>
<td>Transit data confidentiality and authentication is guaranteed by means of “bulk encryption” techniques (end-to-end link encryption) or “network encryption” (end-to-end encryption, usually through network level tunneling techniques like IPSec)</td>
</tr>
<tr>
<td>Border security (firewalling)</td>
<td>Supported</td>
<td>It is possible to define access level network policies</td>
</tr>
<tr>
<td>Transmission infrastructure and link ownership</td>
<td>Internal to the organization</td>
<td>Minimum number of leased lines admitted if supplied by different providers with different networks</td>
</tr>
<tr>
<td>Switching infrastructure ownership</td>
<td>Internal to the organization</td>
<td>No derogation admitted</td>
</tr>
<tr>
<td>Management infrastructure ownership</td>
<td>Internal to the organization</td>
<td>No derogation admitted</td>
</tr>
<tr>
<td>Security infrastructure ownership</td>
<td>Internal to the organization</td>
<td>No derogation admitted</td>
</tr>
</tbody>
</table>

Table 9: main characteristics of a Maximum Security Network (cont.)
3.2.2.5.1.2 Secure Networks

Secure Networks are distinguished from Maximum Security Networks mainly because they admit a connection, although “protected”, with networks having a lower security level.

Another distinctive and significant element is represented by the use of transmission, switching and management infrastructures which are not necessarily internal to the organization.

The main characteristics of a secure network example are shown in Table 10.

3.2.2.5.1.3 Robust Networks

They represent the lowest Secure Network level since they accept that the Network operates in an “Open World” environment.

The main characteristics of a robust network example are shown in Table 11.

3.2.2.5.2 Network Topology – Connectivity

With reference to network topology, the “security” concept should be interpreted as “reliability”.

The fundamental network reliability parameter is its Connectivity level defined as the $K$ parameter, calculated as follows:

$$K = \min_N \{k(n)\}$$

Where

- $N$ is the set of network nodes
- $n$ is the generic node
- $k(n)$ is the number of nodes directly connected to the node $n$
<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Reference Values or Terms</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity</td>
<td>K=2 for access to main locations, k&gt;2 for backbone</td>
<td>Implemented using differentiated physical paths (priority criterion) and/or different nature transmission media (secondary criterion)</td>
</tr>
<tr>
<td>Availability</td>
<td>&gt;99.99% node-to-node (for each node pair) for the backbone; &gt;99.9% end-to-end (for each end-point pair)</td>
<td>Calculated on the basis of MTBF; MTTR and connectivity under normal operating conditions</td>
</tr>
<tr>
<td>Operating non-availability</td>
<td>1 hr</td>
<td>over one year period</td>
</tr>
<tr>
<td>Traffic-based sizing</td>
<td>Project yield performance equal to 80% on the estimated traffic peak</td>
<td>Maximum estimated traffic flow requires 80% of resources in terms of bandwidth use; the remaining 20% of resources remain available to take up other possible overloads</td>
</tr>
<tr>
<td>QoS level differentiation</td>
<td>Supported</td>
<td>By connection</td>
</tr>
<tr>
<td>Priority and pre-emption</td>
<td>Supported</td>
<td>Priority definable at multiple levels (MLPP)</td>
</tr>
<tr>
<td>Information security level and transmission resource routing</td>
<td>Supported</td>
<td>Automatically adapted on the basis of connection. Derived from the military industry</td>
</tr>
<tr>
<td>Integrity</td>
<td>Optional</td>
<td>Recommended</td>
</tr>
<tr>
<td>Graceful degradation</td>
<td>70% service exploitation guaranteed with 80% network functioning; 60% guaranteed service with up to 50% network functioning; no guarantee other than best possible effort for essential services and for services beyond 50% network degradation (e.g. NATO MINIMIZE, situation where the network only routes the traffic from a specific priority level and stops lower priority traffic)</td>
<td>The functioning rate is generally measured in terms of residual/nominal bandwidth over the sum of all backbone network connections. In case one switching node is out of service, all links connected to that node are considered to be out of service. The degradation percentage is the value that makes up 100% of the functioning rate.</td>
</tr>
</tbody>
</table>

*Table 10: main characteristics of a Secure Network*
<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Reference Values or Terms</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible multi-protocol traffic (ATM, IP, MPLS, others)</td>
<td>Strongly recommended</td>
<td>Considered essential in case of highly probable cyber attacks</td>
</tr>
<tr>
<td>Federation with other networks with the same security level</td>
<td>Accepted</td>
<td>It must be a priori foreseen and planned</td>
</tr>
<tr>
<td>Gateways to Internet and other networks with different security levels</td>
<td>Firewall-protected</td>
<td>No derogation admitted to firewall and other protection tools usage</td>
</tr>
<tr>
<td>Secure radio link or wireless access component</td>
<td>Supported</td>
<td>Strongly recommended, eventually as wired link backup solution</td>
</tr>
<tr>
<td>Radio link transit component</td>
<td>Optional</td>
<td>Recommended</td>
</tr>
<tr>
<td>Satellite access component</td>
<td>Optional</td>
<td>Recommended</td>
</tr>
<tr>
<td>Satellite transit component</td>
<td>Optional</td>
<td>Strongly recommended</td>
</tr>
<tr>
<td>Deployable component (deployable/transportable over the territory)</td>
<td>Generally present</td>
<td>Mandatory in the case of an Organization that should support provision of public services in case of disasters. It can include a deployable satellite access component.</td>
</tr>
<tr>
<td>Transit data encryption</td>
<td>Present</td>
<td>Transit data confidentiality and authentication is guaranteed by means of “bulk encryption” techniques (point-to-point link-level encryption) or “network encryption” (end-to-end encryption, usually through network level tunneling techniques like IPSec)</td>
</tr>
<tr>
<td>Border security (firewalling)</td>
<td>Supported</td>
<td>It is possible to define access level network policies</td>
</tr>
<tr>
<td>Transmission infrastructure and line ownership</td>
<td>Not necessarily internal to the organization</td>
<td>Minimum number of leased lines admitted if supplied by different providers with different networks</td>
</tr>
<tr>
<td>Switching infrastructure ownership</td>
<td>Better if internal to the organization</td>
<td></td>
</tr>
<tr>
<td>Management infrastructure ownership</td>
<td>Better if internal to the organization</td>
<td></td>
</tr>
<tr>
<td>Security infrastructure ownership</td>
<td>Internal to the organization</td>
<td>No derogation admitted</td>
</tr>
</tbody>
</table>

Table 10: main characteristics of a Secure Network (cont.)
<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Reference Values or Terms</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity</td>
<td>k&gt;2 for backbone</td>
<td>Implemented using differentiated physical paths (priority criterion) and/or different nature transmission media (secondary criterion)</td>
</tr>
<tr>
<td>Availability</td>
<td>&gt;99.9 end-to-end (for each end-point pair)</td>
<td>Calculated on the basis of MTBF, MTTR and connectivity under normal operating conditions</td>
</tr>
<tr>
<td>Operating non-availability</td>
<td>10 hrs</td>
<td>over one year period</td>
</tr>
<tr>
<td>Traffic-based sizing</td>
<td>Project yield performance equal to 90% on the estimated traffic peak</td>
<td>Maximum estimated traffic flow requires 90% of resources in terms of bandwidth use; the remaining 10% of resources remain available to take up other possible overloads</td>
</tr>
<tr>
<td>QoS level differentiation</td>
<td>Supported, at least on traffic types</td>
<td>Better if by connection</td>
</tr>
<tr>
<td>Priority and pre-emption</td>
<td>Strongly recommended</td>
<td>Priority definable at multiple levels (MLPP)</td>
</tr>
<tr>
<td>Information security level and</td>
<td>Strongly recommended</td>
<td>Automatically adapted on the basis of connection. Derived from the military industry</td>
</tr>
<tr>
<td>transmission resource routing</td>
<td>Strongly recommended</td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>Optional</td>
<td>Recommended</td>
</tr>
<tr>
<td>Graceful degradation</td>
<td>70% service exploitation guaranteed with 80% network functioning; 60% guaranteed service with up to 50% network functioning; no guarantee other than best possible effort for essential services and for services beyond 50% network degradation (e.g. NATO MINIMIZE, situation where the network only routes the traffic from a specific priority level and stops lower priority traffic)</td>
<td>The functioning rate is generally measured in terms of residual/nominal bandwidth over the sum of all backbone network connections. In case one switching node is out of service, all links connected to that node are considered to be out of service. The degradation percentage is the value that makes up 100% of the functioning rate.</td>
</tr>
</tbody>
</table>

*Table11: main characteristics of a Robust Network*
<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Reference Values or Terms</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible multi-protocol traffic (ATM, IP, MPLS, others)</td>
<td>Optional</td>
<td>Strongly recommended</td>
</tr>
<tr>
<td>Federation with other networks with the same security level</td>
<td>Accepted</td>
<td>No derogation admitted for the use of firewalls and protection tools; a “demilitarized” zone (DMZ) can be implemented</td>
</tr>
<tr>
<td>Gateways to Internet and other networks with different security levels</td>
<td>Firewall-protected</td>
<td>Strongly recommended, eventually as wired link backup solution</td>
</tr>
<tr>
<td>Secure radio link or wireless access component</td>
<td>Generally present</td>
<td>Strongly recommended, eventually as wired link backup solution</td>
</tr>
<tr>
<td>Radio link transit component</td>
<td>Optional</td>
<td>Mandatory in the case of an Organization that should support provision of public services in case of disasters. It can include a deployable satellite access component.</td>
</tr>
<tr>
<td>Satellite access component</td>
<td>Optional</td>
<td>Mandatory in the case of an Organization that should support provision of public services in case of disasters. It can include a deployable satellite access component.</td>
</tr>
<tr>
<td>Satellite transit component</td>
<td>Optional</td>
<td>Mandatory in the case of an Organization that should support provision of public services in case of disasters. It can include a deployable satellite access component.</td>
</tr>
<tr>
<td>Deployable component (deployable/transportable over the territory)</td>
<td>Optional</td>
<td>Mandatory in the case of an Organization that should support provision of public services in case of disasters. It can include a deployable satellite access component.</td>
</tr>
<tr>
<td>Transit data encryption</td>
<td>Supported</td>
<td>Transit data confidentiality and authentication is guaranteed by means of “bulk encryption” techniques(point-to-point link-level encryption) or “network encryption” (end-to-end encryption, usually through network level tunneling techniques like IPSec)</td>
</tr>
<tr>
<td>Border security (firewalling)</td>
<td>Supported</td>
<td>It is possible to define access level network policies</td>
</tr>
<tr>
<td>Transmission infrastructure and line ownership</td>
<td>Not necessarily internal to the organization</td>
<td>Minimum number of leased lines admitted if supplied by different providers with different networks</td>
</tr>
<tr>
<td>Switching infrastructure ownership</td>
<td>Not necessarily internal to the organization</td>
<td>Minimum number of leased lines admitted if supplied by different providers with different networks</td>
</tr>
<tr>
<td>Management infrastructure ownership</td>
<td>Not necessarily internal to the organization</td>
<td>Minimum number of leased lines admitted if supplied by different providers with different networks</td>
</tr>
<tr>
<td>Security infrastructure ownership</td>
<td>Better if internal to the organization</td>
<td>Minimum number of leased lines admitted if supplied by different providers with different networks</td>
</tr>
</tbody>
</table>

Table 11: main characteristics of a Robust Network (cont.)
The more connected the network, the more reliable it will be, the other factors contributing to the system’s reliability being equal.

The measure of a network connectivity level is given by the number of nodes a general node is connected to and it is a good rule that in any network, $K$ is sufficiently big and, in any case, at least $K \geq 2$.

A sufficient value for the backbone component of a secure network is $K=3$, corresponding to a network that is able to keep its global connectivity also in the case of two concomitant and in any case displaced failures on the same number of connections.

As to the network peripheral area, that is its access component, it is a good rule the most important access nodes are connected to two nodes belonging to the transit backbone. This is the so called “double homing” technique, also used in public telecommunication networks. A sufficient value for the secure network access component is $K=2$.

Fig. 12 shows a network where transit nodes, indicated with $N_i$, are $K$ connected with $K = 2$ and access nodes, indicated with $M_j$, are double homing connected with the transit backbone.
Please note that $K$ is equal to 2, even if
\[ k(N4) = 5 \text{ and } k(N1) = k(N2) = k(N6) = 3. \]

The aforementioned concepts apply to physical networks as well as to the “higher level” logical networks: this is why security deriving from network topology in considered a “cross-network” characteristic with respect to the physical network and logical network security criteria.

Clearly high connectivity, double homing and every other topological and structural feature increasing the survival degree of a network should be found at each network level, starting from the physical level.

For this reason, a physical path distinction made at the geographical level or with different physical media is certainly recommended.

### 3.2.2.2.5.3 Network federation

#### 3.2.2.2.5.3.1 Preamble

This paragraph describes a distinction between the Network Interoperability and Network Federation concepts.

The **Interoperability between two Networks** $(A \leftrightarrow B)$ integrates the two networks in a situation where:

- the Network A users can connect with the Network B users and vice versa

- Network A users can access database on Network B and vice versa, thus merging the two networks into one single structure.

The **Network Federation**’s purpose is to increase connectivity and transmission capacity in case of emergency through appropriate network links that normally operate separately.

No users and databases connection between the two networks is established.

In other words, the **Network Federation** consists in connect-
ing two or more normally independent networks so that one network (network A in Fig. 13) can use part of the other network to correctly operate its own service.

This way, in an emergency situation Critical Infrastructures can rely on a wide connectivity, theoretically centered on all national “legacy” networks.

Potentially, Legacy Networks may be theoretically represented by:

- network supporting Critical Infrastructures
- PSTN-like communication networks
- wireless communication networks
- military and paramilitary networks
- national distributed networks of public and private structures (broadcaster, satellite TV, Government Networks, etc.)

The Network Federation is therefore limited to connectivity aspects and does not deal with nor grants Network Interoperability.

A Network Federation is possible only if the networks to be included in the federation have a “network supervision” capability and are able to “manage” information routing priorities.
3.2.2.5.3.2 Federation agent

The main entity involved in a Network Federation is the «Federation Agent» who shall:

a) Connect the Networks (from A to B)

The connection is always prepared in advance, but it is utilized only in case of emergency that is identified as potentially able to hinder the functioning of one or more Critical Infrastructures.

To make this operation mode possible, the owners of the interested networks must have entered an agreement providing for such mutual support and, following an emergency, a network accepts to decrease its non essential service to support the essential service requested by the other network.

The presence of a suitable number of Federation Agents is recommended in order to guarantee connectivity between networks of at least $K=3$.

b) Interfacing Networks

The Federation Agent shall operate as an interface (HW, Transport and Standard) between the two networks, by accepting data from Network A and making them compatible with the Network B “environment”.

Indeed the Federation Agent is seen by Network B as a user generating data that must be transferred to other users on Network B (represented by other Federation Agents) that bring back these data to Network A.

c) Managing Priorities

Network A, subject to an emergency situation, through its supervision system and its priority management capability,
identifies the anomalous situation, quantifies it and identifies the support it needs from federated networks.

Then it organized strategic (critical) data and supplies them to the Federation Agents that routes them towards network B that manages them as high priority data (or as data with a pre-arranged priority level).

This does not exclude that, if possible and if accepted by Network B, the Federation Agent also routes the other data as secure data.

d) Managing Security

It is highly recommended that the Federation Agent is able to provide “end-to-end” encryption between the nodes represented by the Federation Agents.

Other characteristics of networks in a federation:

- The networks should be able to manage data priorities
- It is recommended that networks are homogeneous in terms of guaranteed security levels.

As to this last aspect, with reference to Secure Networks and Robust Networks only, emergency has higher priority compared to security guarantee.

Consequently, for these networks it is advisable that a federation is formed also with networks with non homogeneous security levels even if it is believed that the activation of Federation Agents should be first implemented, whenever possible, between Networks having homogeneous security levels.

From this point of view, it is excluded that Maximum Security Networks may be “federated” with networks having a lower security level.
3.2.2.5.4 Network Access – Network Port

The regulation of network access services is one of the important aspects of a good security system that must be taken into account when designing CII networks that must be interconnected with external networks or other CII networks.

A CII Network Port (NP) is defined as the logical access component between the domain or site of an individual user and the CII infrastructure: the definition applies also in case of access to interconnection infrastructure of several CIIs.

The Network Port ensures:

• The connectivity service by interfacing specific access components (wired, satellite, radio link)

• Proper security services.

The concept of Network Port applies to the following types of nodes:

• **Fixed**: where the node communication infrastructures are installed in a building with a fixed configuration, the environment is conditioned and protected

• **Transportable**: where the node communication infrastructures are installed at a site with a semi-fixed configuration, which means that it is possible, having available means and time, to uninstall devices, transport and install them at a different site

• **Mobile**: where the node communication infrastructures are installed in shelters/containers and are fed and conditioned by dedicated devices. As to antennas, a field installation or an installation of the shelters themselves is feasible

• **Vehicular**: where transmission/reception radio equipments are installed on vehicles for the transport of people or goods (cars, land rovers, trucks,...).

The number of services offered over the Network Port can vary in relation to the individual site/user requirements and characteristics.
The Network Port is therefore made of one or more physical components, according to the number of services and their integration level on the same device.

*Fig. 14* summarizes the position of the Network Port.

![Network Port Diagram](image)

The security services provided at the Network Port level, with specific reference to a communication infrastructure based on the IP protocol, are generally the following:

- Traffic flow protection and access control
- Boundary security
- Network intrusion detection systems
- Host intrusion detection systems
- Antivirus and content control systems.

**The Traffic Flow Protection and Access Control** objectives are:

- *Data Origin Authentication:* verifies the authenticity of the send-
ing node of each IP datagram

- **Data integrity**: verifies that each datagram content has not been changed (deliberately or due to line errors) during the transit from source to destination

- **Data confidentiality**: hides the text contained in message by means of encryption

- **Replay protection**: ensures that a hacker, having intercepted an IP datagram, is not able, a posteriori, to send it back to the destination for illegal purposes.

For the *Traffic flow protection* for example the IPSec protocol, integral part of the new version of the IP protocol (IPv6) which can also be used with IPv4, represents an open architecture, defined by the IPSec Working Group of IETF (RFC 2401), and is the more general protection solution (encryption/integrity/authentication) for the data transmission over a network. The IPSec protocol can be used as an end-to-end solution, which protects the information exchange directly between communication sender and receiver, or it can intervene between two intermediate systems acting as security gateway, as it happens in the implementation of virtual private network. Being at the network level, IPSec is a very general solution (can protect the whole IP traffic) and is application transparent.

The Network Port can use both standard and proprietary encryption algorithms (DES, 3-DES, RSA,...).

Encryption keys of suitable length are used to ensure “robustness” for both Confidentiality (*Strong Encryption*) and Authentication (*Strong Authentication*).

The authentication mechanism generally uses Asymmetric Keys and X509 Digital Certificate, thus enabling integration of the service in a PKI structure.

As to access control, since a digital certificate validation is a function that has a significant impact on the total performance of a PKI infrastructure, the IETF OCSP (On Line Certificate Status Protocol) standard allows the use of digital certificate for data source
authentication, in particular the real time certification type (RTC = Real Time Certification) and the activation of the access control service between:

- site “a” Network Port and site “b” Network Port
- Stand-alone workstations and Network Port at a site

The **Logical boundary security** service objectives are to guarantee the following:

- **Firewalling**: this service implements the traditional functionalities of traffic filtering, permission policy management (for example, “Deny any service expect those explicitly permitted”), etc, keeping auditing and logging of traffic through the firewall.

This type of service can also be supplied separately for:

- The traffic from the CII to the Network Port (and vice versa)
- The traffic from the User Network and the environment were the Network
- Port is installed, as in the case of specific Servers (for example Management, Middleware servers, …) on a “DMZ” downhill the Network Port.

- **Denial of Service (DOS) attack protection**: the service contributes to increase the communication system security, both in terms of service Availability and Continuity, by preventing *cyber attacks* aimed at causing the impossibility to use IT resources.

The **network intrusion detection** service activates and manages intrusion detection systems (called *Network Intrusion Detection System* - NIDS), whose functioning is based on their ability to observe network traffic. An NIDS is a hardware/software configuration, with one or more (sensor) systems installed on the networks in order to:

- identify all attacks against the network they are intended to protect
- identify all situations where there is no attack against the network they are intended to protect.
The service makes it possible to:

• protect IT assets

• identify and fix possible network vulnerabilities in a short period of time

• collect and keep accurate log of the attacks occurred in order to favor the identification of the attack perpetrators and as a deterrent to discourage further hostile actions.

The service is equipped with a NIDS Management component that makes it possible to:

• obtain information on attacks from the information sources ("sensors") located on the network

• perform a predefined analysis of detected events

• trigger a specific notification when an attack is identified

The host intrusion detection service activates and manages intrusion detection systems on the hosts (called Host Intrusion Detection System - NIDS), whose functioning is based on their ability to observe information taken from the hosts they are intended to protect.

A HIDS is software installed on a host in order to:

• identify all attacks against the host it is intended to protect

• identify all situations where there is no attack against to the host to be protected.

The service, provided with a Management component, allows to:

• protect workstations and server systems

• identify and fix possible host vulnerabilities in a short period of time

• collect and keep accurate log of the attacks occurred in order to favor the identification of the attack perpetrators and as a deterrent to discourage further hostile actions
trigger specific reaction when an attack is identified.

The **antivirus and content control** service implements and manages a protection system of possible application servers (installed at the Network Port) from harmful codes. The “harmful code” term indicates any type of executable software code (Virus, Worm, Trojan, etc.) that might damage the IT environment intentionally or not intentionally.

Also this service allows the central management of antivirus software installed on a portion of or all the machines of the information system intended to become secure.

### 3.2.2.2.5.5 Security Structure at the Middleware - Application – Procedure level

The CII network security cannot leave aside a middleware, a data and application management software and an organizational level security infrastructure that also includes ad hoc procedures that all staff accessing and using the system must apply.

First of all, it is necessary to check whether the operating systems and software used for CII networks meet the security certification standard requirements, are the most recent versions and are constantly updated.

One of the most important functionalities at all levels (client, middleware and data server) is **authentication**, that is the possibility to uniquely identify the subjects operating on the system.

It is therefore possible to define different levels of access to the system and its resources on the basis of individual users’ profile and characteristics; every system service check the credentials provided and, on the basis of Access Control Lists (ACL), provides correct resource access (e.g. read only, read and write, no permission, etc). As to the systems whose data are particularly sensitive, the application of these access criteria should directly be provided by the **kernel** of the database manager rather than at the application level. Only this way, it is therefore possible to avert the risk of unwanted accesses that might
bypass the controls performed by the applications.

The user authentication functionality can be, for example, implemented through a Public Key Infrastructure (PKI) architecture with a (technological) Certification Authority that is able to generate X.509 Digital Certificate for each user, application and service that must be authenticated in the system (also for Network devices).

*Fig. 15* shows a very general PKI architecture with different players interacting with other PKIs.

- The main PKI components are:
  - Certification Authority (CA): responsible for issuing and revoking Digital Certificates
  - Registration Authority (RA): responsible for checking the information that associates a public key to the entity that will use it (that can be different from the one requesting a Digital Certificate)
• Digital Certificate Holder: person, hardware device, software agent representing the entity that will use the public key (that is the Digital Certificate) to prove its own identity

• Digital Certificate User: person, hardware device, software agent that validates an authentication starting from a CA public key (Digital Certificate)

Certificates and lists of revoked certificates are stored and published in ad hoc repository. The operating and interaction model of the various PKI players is summarized in Fig. 16:

![Fig. 16: PKI Operating Model](image)

The PKI user requests the RA to receive a Digital Certificate. The RA, after checking all data and performing the steps provided for by the PKI management protocol, asks the CA to issue the Digital Certificate. The CA issues the Digital Certificate to the user and publishes it in the public Repository.
The PKI end users can use all encryption, Digital Signature, Hashing functions made available by the PKI, using their Digital Certificate and those of other users with whom they want to interact by recovering them from the Certificate Repository.

This repository should be implemented following appropriate security precautions.

During the PKI Management and Administration operations revocation of Digital Certificates may be requested to the various RA for users who are no longer trusted by the PKI. The CA will carry out revocations by invalidating Digital Certificates and issuing a Certification Revocation List (CRL) that is published in the Repository. Every end user, before authenticating a Digital Certificate received, should check that it is not included in the published CRLs.

To manage the CA Policy one or more Certification Authority Operator (CAO) are used, whilst to manage digital certificate requests from users one or more Registration Authority (RA) are used also via the Web to make it possible to generate requests from the Web Browser of the user’s workstation.

To solve the problem of the size of the certificates present in the CRL system, the OCSP protocol can be used. It allows to:

- send only information on the status of the certificate in question (and not of the whole list)
- interact with the Certification Authority (CA) issuing the CRLs
- enable a centralized management of the certificate status.

More specifically, to achieve high performance and high reliability levels, it is possible to use a distributed OCSP system (D-OCSP) that provides good protection against DoS attacks and is not vulnerable to intrusion attacks. The D-OCSP system also allows:

- *Effective scalability* by separating the validation process from the security operations associated with the certificate validation process.
- *High reliability* thanks to the fact that end users’ applications connect to a local LDAP server
• High performance achieved thanks to a reduced distance between the user application and the Repositories

• High availability because possible multiple attacks to prevent the service are virtually eliminated through the use of multiple Repositories geographically scattered

• Cost optimization since Repositories do not require secure communication, positions or operating modalities and the costs associated to their large scale distributed are minimum

• Flexibility and adaptability: each Repository can support more than one CA with the consequent possibility to have total control over its domain

• High distribution capacity: repositories can be distributed everywhere without hindering performance due to network slowdowns

• Better environmental factors: since Repositories do not contain any sensitive data for security purposes, they can be located in environments where there is a real threat of attack

• Ideal architecture for scenarios subject to sudden changes: since it is possible to easily and quickly add or eliminate Repositories

• High security because two important security factors have been improved compared to traditional OCSP systems:
  - The certificate validity requests only to go to responders, rather than to validation authorities. Since validation authorities do not allow any incoming communication from the external world, the threat of an external attack is virtually eliminated
  - An extension of the validity structure to adjust it to a growing number of users does not require a corresponding additional distribution of sensitive data and secure applications. Consequently the capacity to securely manage these operations is remarkably improved.

The system requires one or more Time Stamp Servers so as to implement the necessary Time Stamping service for the Digital Signa-
ture and Non-Repudiation functionalities.

The Certification Authority does not necessarily have to be connected to the CNI network (in order to avoid external attacks).

The PKI system gives all system users a library of functions that is interfaced with the applications (that can be Web Oriented, email Client and ad-hoc developed applications), enabling document hashing, encryption, digital signature, information retrieval from the reference LDAP server (e.g. CRL, Digital Certificates and public keys of other users, services, …).

Each PKI user should have a device to store his/her own Private Key and Digital Certificate. This device should have security characteristics that do not allow the loss (or cloning) of the private key that enables all PKY operations (encryption, digital signature,…).

As to software services (for example the Certification Authority itself) the private keys are stored in the so-called Hardware Security Modules (HSM) that also allow to back-up the private key in a secure manner (should the CA private key be lost, the entire PKI would be invalidated).

Fig. 17: PKI Architecture
Each PKI end user is given a Smart Card (for example, the CMD Multi-service Card of the Department of Defense) through which users can authenticate to the system (also through biometric functionalities: digital fingerprint) and interact with the PKI (on the Smart Card, a private key of the user’s Digital Certificate is generated and stored).

Only a Smart Card reader on the user’s workstation is necessary.

On the LDAP Server, besides Digital Certificates and public keys, also user profiles are stored so that they are filed within different Organizational Units (OU) and are granted different network, service and application access rights.

All services and applications, once the communication counterpart is authenticated through the services offered by the PKI, check the user profile and apply their own resources Access Control List (ACL) to the user.

An important functionality that can be obtained with a PKI is the Single-Sign-On that allows users to be authenticated to the system with one credential only (the one supplied by the digital certificate) and they are able to access all resources through correct profiles and permissions.

The user does no longer have different mechanisms to logon to resources (i.e. different usernames and passwords for each system).

Another important functionality is, therefore, access control that is provided with better security features whenever real time solutions (RTC) and distributed certificate validity systems (D-OCSP) are used to serve hundreds of thousands users, ensuring great reliability, high performance, security, and minimum implementation costs.

The RTC system employs the distributed validation architecture described in Fig. 18 and supports both digital signature checks and self-validating check such as V-Token, CRL or Mini-CRL.
3.2.3 Network power supply systems

The power supply for an electrical network represents the primary power source of CII telecommunications systems and their correct operation directly depends on its continuous availability.

Taking for granted that the primary power supply source is provided by one or more specific operators, a correct definition of the service levels guaranteed under normal conditions and the terms of intervention and collaboration in case of emergency is necessary.

During normal system operation, the provision conditions are regulated by specific service agreements, in case of emergency the entire power supply autonomy of the network or infrastructure operator should be pursued, by assessing the critical capacity and the duration of the autonomous operation.

Clearly the availability of an end-to-end service also in the case of catastrophic events depends on the real available autonomous solutions for all the elements involved in the information flow.

The real availability should be measured taking into account the weakest element in the chain: for example, it is possible to assume

![Fig. 18: Distributed RTC Architecture](image_url)
that a data center has a power generator that can ensure some days of autonomy in case of emergency; it is unthinkable to extend this solution to all the remaining nodes of the network infrastructure. Anyway, these require less costly solutions that ensure appropriate autonomy.

All network and node systems are sensitive to changes in the power supply components and should be equipped with appropriate filtering and incoming energy stabilization systems. Furthermore, appropriate protection against micro-supply interruptions or against temporary voltage drops should be provided.

### 3.2.3.1 standby systems

In case of suspension of power supply on the part of the primary power provider, emergency generators should start operating with no interruptions and when normal conditions are restored, they should be excluded in a completely transparent manner.

All systems should be equipped with manual starting procedures in case the automatic activation fails.

With specific reference to electrical generators, the availability of autonomous electric power generation is a function of the capacity of fuel tanks, of the generator efficiency and of the quantity of energy necessary to operate the systems.

The autonomy level shall be higher whenever climate conditions, for example, do no require full use of air conditioning systems and it will be lower in the opposite case.

Autonomous production systems should be redundant and sized according to the operating requirements.

All non indispensable systems should be excluded from the autonomous energy supply system to avoid reducing the endurance time.

It is important to define fuel supplying policies during emergencies, also resorting to available alternative suppliers.

A gradual exclusion plan for non indispensable loads to ensure continuous supply to vital systems should exist.
3.2.4 Data Centre Security issues

Data Centers, that is the physical environments where IT systems and infrastructures are installed, represent a particularly sensitive element for the continuous functioning of a Critical Infrastructure.

In many cases these are rooms that were not specifically designed for this purpose and are the result of technological adjustments in buildings designed for different purposes, with clear structural and logistic gaps and limitations.

The events following the September 2001 attacks have shown how new risk factors call for suitable physical infrastructures.

3.2.4.1 Environment and borders

The specific Data Centre location in the territory should take into account risk factors related to:

* the natural environment (seismicity of the territory, risk of flooding or seakes)
* Neighboring reality that might represent a direct threat or a harmful event amplifier (fuel storage, harmful processing, chemical industries, etc.)
* possible targets of specific attacks (military installations)
* possible critical factors in case of emergency (high audience density sports premises or theatres)

The location may affect the availability/continuity of primary production factor supply (e.g. the vicinity of large industrial plants may strongly impact electric power supply) or emergency operators’ or teams access.

3.2.4.2 Building structure

The building should be specifically designed to ensure appropriate distribution of technological and structural systems and to make the environment easily defendable or manageable in case of emergency.
When refurbishing and/or adjusting existing infrastructures, all systems and the physical distribution of spaces should be re-designed and correctly sized.

The structure should be divided into “water-tight areas” to limit and confine damages to well-defined areas.

The external structure should be defendable against armed attacks, walled and supervised and should not host other entities or services.

Above the ground buildings should not shelter garages, vehicles or deposits unless it is strictly necessary for the Data Centre functioning.

The structure should only have the strictly necessary access points (people and goods) and avoid direct drives that might facilitate breakthrough attempts.

The location should be rapidly and easily reached by rescue teams in case of accident and should have wide room for maneuver.

In case of unavailable primary access ways, there should be an alternative access and evacuation path.

### 3.2.4.3 Technological plants

#### 3.2.4.3.1 Local Loop

Access to TLC networks should be through physical paths that are distinct and redundant so as to guarantee continuity of service in case of events that might make the system or one access way unusable, accidentally or for security reasons.

#### 3.2.4.3.2 Electrical system

Particular attention should be paid to designing, sizing electric power supply system and its continuity.

The whole production and distribution system should be redundant, possibly in opposite areas of the building.
The Data Centre should be equipped with suitable autonomous generators that are able to ensure functioning also in case of a prolonged suspension of the main power supply system.

Periodic accident simulations and auxiliary and redundant system tests should be provided for and regulated.

standby systems, batteries and other industrial electrical system structural elements are specific fire risk factors that should be carefully assessed and neutralized.

3.2.4.3.3. Air conditioning system

Similar attention should be paid to designing, sizing the air conditioning system and its continuity: keeping the appropriate temperature is indeed necessary for the correct functioning of the systems.

The use of miniature and highly concentrated IT components reduces the physical room taken by said components, but it increases the concentration and quantity of heat developed by the systems. This requires that cooling is managed by means of flexible distribution factors and with different loads according to the different Data Centre areas, in terms of air conditioned supply and the removal of warm air.

Air conditioning side effects should be assessed and neutralized (vibration, dusts, water leakage).

3.2.4.3.2 Fire system

The same precautions should be taken when designing, sizing the fire detection and fighting system and its continuity.

Possible fire extinguishing actions in subsequent waves should be possible to avoid revamping of fire.

Protection against fire is also the result of specific structural choices (hence the advantage of having specifically designed areas) such as lack of windows, the possibility to contain fire in the various sections of the building, absence of inflammable materials in the
premises and the presence of insulating materials and false ceilings.

All rooms with possible risk factors (electrical power plants, deposits, etc.) should be separate and away from operating areas where processing systems are located.

Periodic fire simulations should be provided for and regulated for the personnel involved.

### 3.2.4.3.5 Access control

People access to the rooms should be rigorously controlled by means of personal identification, continuous remote surveillance and, whenever necessary, direct escorting of external personnel.

All accesses should always be tracked.

In case of emergency, quick access releasing procedures should be provided for rescue operators.

### 3.2.4.3.6 Monitoring and alarm systems

All infrastructure systems must be equipped with appropriate monitoring and alarm systems with automatic escalation procedures according to the detected dangerousness factors.

### 3.2.4.4 Emergency procedures training for the staff

All staff should be specifically trained on the structure access and use modalities as well as on all emergency procedures even if they do not directly fall within their competence.

Emergency procedures documentation and summary schemes should be kept in all operating areas to enable intervention also of staff that is not specifically in charge.
3.2.5 Emergency Networks

Emergency networks are generally defined as networks that are not able to support transmission of data (Normal, Secure or Strategic) necessary for the correct functioning of the Critical Infrastructure. However these networks are able to report to a Control Centre (at the Critical Infrastructure or at the national level) the Critical Infrastructure condition (data and/or voice).

These networks are considered as a last resort to inform a higher body about the infrastructure status (generally causes and damages that led to the crisis that is preventing information transmission by means of the systems provided, for both lack of transmission capacity and lack of a network).

An example of emergency network implementation is an HF (2-30 MHz) band radiofrequency network.

An HF networks is created by means of HF transceivers and consequently both Access and Transport functions are radio based.

The bandwidth that can be used for information transmission (voice or data) purposes is around 3 MHz (corresponding to approximately 3 Kbit/sec) and the system is able to support both analog (voice and data) and digital (voice and data) transmissions.

Ranges vary from tens of kilometers (earth waves) to hundreds of thousands of kilometers (sky wave that exploits the reflection of the high layers of the atmosphere) and are highly affected by meteorological conditions and by the time of the day (attenuation changes around 90 dB are experienced).

For this reason, the use of the lower HF band is strongly recommended so as to be operating 24 hours, for example, in August with a high solar emission activity.

The network access can be operated by a simple hand held radio system or by more powerful fixed radio terminals.

The HF Emergency Network should be able to provide:

- Emergency Frequencies to distribute information to all users and establish a connection other than the planned ones
• a user frequency assignment and usage plan

• a sophisticated Supervision and information re-routing system that takes into account the “current” availability of fixed stations that represent the network nodes

• a direct support to communication between users by using local, regional and national connections, only based on mobile systems.
3.3 MANAGEMENT AND ORGANIZATIONAL ISSUES

In the present paragraph, we will analyze, always from the perspective of Good Rules, the main organizational aspects that concern the management of Communication Networks and then we will review some of the technological trends in the area of Secure Networks.

3.3.1 Joint management of crisis situations caused by ICT infrastructures

As already mentioned, critical national infrastructures are managed by a plurality of public and private institutions. The use of ICT technologies has determined such a strong interdependence between critical structures that a damaging event that occurs in one structure can also have an effect on the other structures, causing service disruptions to users who do not have a direct relationship with the infrastructure that has been originally damaged.

Starting from the assumption that every institution should have its own emergency plans/Disaster Recovery/Business Continuity, as prescribed by ISO/IEC 17799/BS7799, every structure should have a Crisis Management Unit (CMU).

Similarly, a Joint Crisis Management Unit (JCMU) should be set up in the context of cooperation between the different institutions.

In order to function properly, this Unit will need to use a matrix of the interdependencies of the services provided by the various companies that will allow to identify, once one or more institutions have been affected by a damaging event, which other structures are involved, the way and the probable time frame in which the effects caused by the damaging event will propagate within the structures, and also when the service disruptions will end. That will also be useful to determine intervention times and to prevent/limit the domino effect.
3.3.1.1 Crisis Unit

The Crisis Unit is the governing body that should oversee the plans for the management of serious emergencies (physical or computer attacks, natural or accidental disasters, serious technology failures, serious organizational problems) that have a strong impact on the ICT structures that support the CII. The Crisis Unit could be activated also in case of disaster forecasts to classify the event and/or for the eventual identification of possible countermeasures. In case of emergency, the Crisis Unit could oversee the following activities:

- evaluation of the situation (alarm management phase)
- realization of the recovery plan (disaster management phase)
- return to normal operating conditions (recovery phase).

3.3.1.2 Identification of the people in charge of CII and ICT emergency management

The first step in the constitution of a JCMU will be the definition of the roles, the identification of the professional figures inside the single institutions/companies that have the necessary decision-making authority and also the definition of the processes. It will therefore be necessary to define procedures that will establish when the state of joint crisis shall be declared and how this state should be managed until normal activity is resumed (Joint Crisis Management Plan, JCMP).

The JCMU will comprise a Coordinator and the representatives of the Crisis Management Units of the single institutions/companies that manage the different critical/ICT infrastructures. It will be possible for a representative of the CMU of the single institution/company to assume the role of JCMU Coordinator and, therefore, this figure will have a double role. (Fig. 19).

The appointment of each JCMU member in the different institutions/companies shall be formalized by the top management of the institution/company and then notified to the Coordinator. The appointment of the Coordinator will be formalized in the same way...
but, in this case, the various institutions/companies will have to agree on the choice of the person and his/her subsequent appointment.

All CMU representatives shall receive real-time information on the situation of any existing emergency inside their own structure.

Each component of the JCMU will have a telephone number where he/she can be reached in case of need and an e-mail address where all informational communications shall be sent. Emergency situations and consequent summons will be reported by phone, and then formalized by e-mail. JCMU members shall always be reachable, also when on vacation, therefore there should be a company telephone number through which it would be always possible to reach the representative of the single CMU or his/her substitute.

A quick and efficient communication between all the members is crucial for the operation of the Unit. Therefore, communication means should be always active and in high availability configuration.
3.3.1.3 Interaction, integration and interoperability modes

Every time the CMU is activated inside a single structure because of an emergency (computer or any other kind of damaging event), the corresponding JCMU representative, using the previously defined matrix of the interdependences, shall be able to:

1) determine the criticality level of the situation
2) make a realistic estimate of the duration of the ongoing service disruptions
3) foresee eventual impacts on the other infrastructures
4) in case of possible external impacts, alert all JCMU components.

Once the JCMU has been convened, it will decide whether to declare the state of Joint Crisis or not. If the crisis is declared, the JCM indications shall be followed and therefore actions shall be taken to avoid the propagation of service disruptions to the infrastructures that have not been affected yet by assisting the other institutions/companies in limiting the effects/damages. If the crisis is not declared, the JCMU will follow the evolution of the situation until the criticality level is lowered and/or the emergency of the infrastructure that has been damaged is declared over. Anyway, in both cases, before the JCMU breaks up, the end of the state of Joint Crisis Management (JCM) must be declared and, at the same time, a document, containing the recording/description of all the management phases of the event, will be prepared for later analysis.

A possible operational flow is represented in Fig. 20.
Fig. 20: Possible operational flow
In order for this flow to achieve optimal results, a risk analysis on the interdependence of the services provided by the different managers of critical and ICT infrastructures must have been previously performed. This analysis must have identified the potential threats/vulnerabilities to which each structure could be exposed in case a damaging event should occur in one or more infrastructures and the probable duration of the consequent service disruptions. Therefore, the countermeasures to be taken in order to avoid the propagation of the emergency/service disruption will have been previously defined.

These analyses could also lead the companies that are part of the JCMU to sign support agreements with the damaged companies.

Whenever, in case of incident, it is possible to avoid the propagation of the service disruptions between the different infrastructures, the JCMU will have to analyze the event and how the emergency has been managed in order to avoid the same situation to happen should the same event occur.

- Therefore, the JCMU shall periodically meet to discuss:
  - the incidents that have occurred in that period
  - how the single institutions have reacted
  - impacts evaluation/damage amount/service disruptions caused by each incident
  - possible solutions to keep the same problems from happening again.

Therefore, in addition to the JCMU, there should be a registry of all the emergencies that have occurred with the details of all the activities that have been carried out.

In case of serious emergency situations, the JCMU shall release information bulletins to update the competent institutional subjects on the situation.

In case of a known threat that is spreading across the different national/world ICT structures (i.e. computer virus), the Coordinator shall summon the members of the Unit to follow the evolution of
the situation, evaluate the precautions/actions that have been taken by each Institution and eventually decide to take a common action to counter the threat.

The JCMU shall also have the task of disseminating information inside each infrastructure and promote initiatives concerning security, the reduction of the effects of eventual damaging events, the subsequent management of the emergency and responses to computer attacks.

In order to enable a proactive management of eventual emergencies, it is essential for JCMU components to exchange information on new threats or potential damaging events. It is therefore advisable that the JCMU would employ Early Warning instruments to obtain such information and Information Sharing tools in order to establish real-time information sharing between the members.

All confidential information on emergency situations that will be exchanged among the JCMU members shall not be disclosed to unauthorized parties.

**3.3.1.4 Joint training activity and support tools**

A cooperative joint crisis management training program will have to be developed for JCMU members.

* The JCMU shall be provided with tools that will allow to:
  * define virtual reality (VR) models that allow to determine the areas that could be affected by an emergency
  * identify possible intervention scenarios
  * determine the key elements for the definition of management strategies
  * define the different training strategies
  * perform a continuous review of the previous topics considering the actual situation in the structures that participate to the JCMU.
Every new JCMU member will have to be trained on the above-mentioned points.

All JCMU members shall have an in-depth knowledge of joint crisis management plan (JCMP) and especially of the parts of the plan that involve them directly.

Every time a fundamental part of the JCMP is modified/updated, the JCMU Coordinator shall summon the members to update/train them on the new JCMP.

Every time there is a modification in a critical infrastructure/ICT platform of any structure that could determine a variation of the matrix of the interdependencies of the services and/or of the JCMP, the members of the JCMU will have to attend an update workshop.

In addition, periodic updating courses shall be held on new methods/strategies for the management of crises caused by emergencies in the different critical/ICT structures and on the new tools that allow forecast/manage the behaviors of these infrastructures in case of incidents.

3.3.1.5 Good rules for ITC emergencies management, including Call Centre

As previously mentioned, ISO/IEC 17799/BS7799 provide all the indications on how to build Business Continuity Management Processes and hence Business Continuity Plans and among them we find:

- identify and agree on every responsibility and emergency procedure
- implement emergency procedures that will allow restoring critical systems/services within predefined time frames in case of emergency
- produce documentation of the agreed emergency management processes/procedures
- adequately train all the personnel involved in crisis management on the above-mentioned processes/procedures
* test and update emergency management plans.

Without these preliminary activities, emergency management could become quite problematic.

Therefore, the following activities could be defined as the minimum actions necessary to manage emergencies:

1. top management approval of a budget to guarantee the operational continuity of critical systems/services
2. institution of a structure (Crisis Management Unit) that will coordinate recovery actions in case of a disaster or a service disruption
3. definition of an adequately documented process (crisis management plan) for the management of emergencies and service recovery
4. periodic tests of the crisis management plan through emergency simulations
5. periodic plan update, also taking into account existing regulations/standards/directions and the processes that are used by the other organizations.

During a crisis, it is important to:

1. follow, as much as possible, the indications of the Crisis Management Plan (CMP)
2. constantly update top management on the state of the crisis
3. assign the highest priority to the procedures that protect people’s safety
4. manage relationships with the media (press, television, radio), avoid providing unnecessary news that could cause panic in the citizens as well as do not suspend communication channels with the public
5. apply every procedure that will allow to avoid/limit the propagation of damages to other organizations
6. try to avoid/limit the image damage of the company that has been hit by the crisis
7. record every information that allows to document the damaging event, its effects and the actions that have been carried out to manage the crisis in order to be able to reconstruct and analyze the whole situation.

In case of joint crisis management, the communication factor is clearly crucial and therefore it is necessary to maintain active contacts with Police Forces, State Institutions, the centers that provide information services to the citizens or to the single infrastructure (information on threats/damages, situations in the territory) and with any other organization that cooperates in the management of the emergency.

Another important factor, in case of emergency situations, is to have the possibility to contact the various Call Centers to receive information/indications on the disruptions of service that have occurred.

The Disaster Recovery/Business Continuity plan of each infrastructure shall, then, include all the activities/processes/procedures that will guarantee the operational continuity of their respective Call Centers. This will enable these structures to provide citizens with useful information about ongoing service disruptions, also using, only if the emergency situation allows it, eventual Web services that have been made available to the users. Clearly, in case of joint Crisis management, the JCMU shall provide the different Call Centers, through the CMU representative of each company, with reliable information on the ongoing situation and on the probable duration of the service disruption.
3.3.1.6 When and how to perform ICT emergency simulations

In order to assess the efficiency of the Joint Crisis Management process also with respect to the technological/organizational evolution of the single infrastructures and, therefore, in order to maintain an adequate preparation/training level of the JCMU members, it will be necessary to periodically perform emergency simulations (at least every six months).

An emergency situation simulation consists in performing all the activities included in the JCMP, for example the convocation of the Unit, the evaluation of impacts, of the eventual escalation and of the length of recovery time to normal activity, the release of communiqués, etc. The simulation, of course, will not include a real system/activity shutdown in any of the infrastructures. In order for the simulation to be realistic, it should be conducted in a joint test environment where everybody has implemented the part that is under their own responsibility and there is a small-scale representation of all ICT and non-ICT critical infrastructures that are used to provide the various services.

It is advisable that the JCMU Coordinator would at least once a year summon every Unit member without previous notice to verify his or her availability and response times.

At the end of each simulation, the results shall be recorded and reviewed and, on the base of this analysis, the JCMU will certify the conformity of the JCMP or eventually review the crisis management processes/procedures (JCMP adjustment) or decide to repeat the simulation.

The simulation tests could also provide useful indications for the single infrastructures.

The use of IDSS (Intelligent Decision Support Systems), and/or of Modeling and Simulation Environments could be useful both for internal training and for the JCMU components for the evaluation of the possible impacts of an incident.
3.3.1.7 Communication issues of Joint Crisis Management

The presence of the JCMU imposes the need for a communications system that will be able to support the Unit’s operations. This Communication Network shall:

• record and provide to the JCMU (both in normal and emergency operational conditions) information on the present state of the infrastructures and a short-medium term forecast with eventual assistance requests concerning both the structure itself and its communications

• Allow the JMCU to send data and information to the Critical Infrastructures to manage the situation and to support their operations

• Allow the JMCU to exchange information with the competent State bodies

• Allow any other information exchange that should become necessary to manage the crisis and minimize damage.

The operations that have to be performed by the JCMU fall under the category of the so-called Network Centric Operations and they need a Network Centric Communications solution that will assure Interoperability between communication networks.

In fact, the above-described data exchange requires the data and the users that are available in the communication network A of Critical Infrastructure A to be accessible (with the users interacting and interchanging data and information) by the JCMU and that the information and data provided by the JCMU should be used by network A’s users.

The solution that could be adopted at the national level is an ad hoc network (Fig. 21) distributed at national level that should interface with:

• every telecommunication network that supports every CII

• every telecommunication network of the competent State bodies
- every telecommunication network of the Crisis Intervention Organizations

and implement the share and exchange of the above-described information. The JCMU communication network:

- will always be connected with the above-mentioned networks
- will not normally consent a direct data exchange between Critical Infrastructures, exchange that will be possible only at the request of the JCMU
- will be secure at the maximum security level because it will handle data that must be always considered critical both for its own nature and for the operation of the JCMU.

Fig. 21: «Ad hoc» national network
3.3.2 National and world trends

3.3.2.1 Technological and Organizational trends

Technological and organizational trends, both at European and World level, are focused on one hand on the search of technological solutions that will guarantee an «intrinsic» security of the Communications Network system through the adoption of new protocols and protected links and, on the other, on the diffusion of «Security» concepts and issues among the various operators through regulations and Best Practices that will allow an «intelligent» use of the existing communications complex by adapting them to the new protection requirements.

In the first chapter, we have mentioned the PARS (Preparatory Action for Research and Security) launched by the European Commission: indeed, 3 out of the 5 areas in which the European «global» protection requirements have been divided concern the new technologies for communication networks, their interoperability and their management according to the «Network Centric Operation» conceptual framework.

The US «Govnet» network is an example of an independent administrative network that integrates the two above-mentioned concepts: it was designed as a private voice and data network based on the Internet Protocol (IP) but without interconnection with commercial and public networks.

3.3.2.1.1 Intelligent SW Agents

Among the latest technologies that can be applied to critical infrastructures communication networks, intelligent agents occupy a prominent place. Intelligent agents, also known as «software agents», can autonomously perform many of the operations usually performed by regular users, in addition to many other tasks.

For example, the multi-agent system architecture RETSINA, developed by the Carnegie Mellon University of Pittsburgh (USA), can be applied to a vast range of domains, such as:
Network interoperability, especially in the field of data access and sharing that are evolving in the direction of «Information Dissemination» in Network Centric Communications

- Logistics planning in military operations
- Personalized information management
- Wireless mobile telecommunications management
- Financial portfolios management
- Internet auctions.

Intelligent SW Agents technology in use in the context of the protection of interdependent critical infrastructures concern both for the development of distributed control systems, as in the case of the SAFEGUARD European project that aims to improve the robustness of the control system of the electrical distribution grid, and also for the critical infrastructures modeling and simulation aspects. At this last regard, we can mention the activities conducted in the United States by NISAC (National Infrastructure Simulation and Analysis Center, the result of an alliance between Los Alamos National Laboratory and Sandia National Laboratories together with other important American research structures) and the CISIA (Critical Infrastructure Simulation by Interdependent Agents) project that is sponsored by a number of Italian Universities¹.

3.3.2.1.2 IPv6 Protocol

With the worldwide proliferation of Internet access, 32 bit technology, on which the currently used IP protocol version 4 (IPv4) is based, is rapidly becoming insufficient.

IPv4, developed over thirty years ago by the US Department of Defense, in fact provides about four billion (equals to $2^{32}$) IP

¹ Specifically by CAMPUS Bio-Medico University of Rome and by Roma Tre University
addresses: despite apparently a very high number, nonetheless it might not be enough to fulfill all Global Network access requests.

Therefore, the need arose for a new 128-bit protocol, initially called IPng (IP next generation) and today known as IPv6.

The benefits introduced by IPv6 are:

- **Exponential growth of available IP addresses** ($2^{128}$): thanks to the new protocol, each node can have its own address.

- **Native IPSec inclusion**: IPSec AH and ESP headers are part of IPv6 Extension Headers. Therefore, now IPSec support is a mandatory feature and not just optional as in the previous version. This favors/encourages the proliferation of

\[ Fig. 22: \text{One application of the RETSINA architecture} \]
secure end-to-end connections. In addition, services such as FTP, IRC, SNMP, H323, SIP and RPC, that were difficult to use with IPv4, are now facilitated.

- **High processing speed**: the datagram header format has been greatly simplified in order to increase the speed of the operations performed by network components.

- **NAT elimination (Network Address Translation)**: the availability of a sufficiently large number of IP addresses allows eliminating NAT, a tool that is used to identify a group of machines through a single public IP address. In addition, the new IP protocol takes full advantage of IPSec’s capabilities.

### 3.3.2.1.3 Smart Communication Nodes

A trend that is shared by all the specialists in the field of operations in complex environments, and in particular in «systems of systems» engineering, is to regard interoperability between existing networks, legacy and new networks (or networks that are updated due to operational requirements) as an operations support in a «Network Centric Communication» conceptual framework.

This evolution is based on three elements: the networking component, the data access and sharing component and the security component.

Smart Communication Nodes represent the evolution of today’s Multi-protocol Switches and are destined to solve «networking» issues in the evolving scenario of network interoperability.

These nodes will be able to route information on different routes operating simultaneously on different transmission protocols and on the different information handling standards thus allowing the integration between non-homogeneous networks and systems and the simultaneous support of different standards and protocols.

Smart nodes, in consideration of their extension to new standards such as IPv6 and VoIP and of their capability of acting also as
Federation Agents, can be the solution for the above-mentioned federation and interoperability issues.

### 3.3.3 The Human Factor

Aside from the technical and technological aspects that have been already extensively discussed in the present document, it is essential to also consider the **human factor**, which represents a crucial element for any ICT security policy.

Part of the vulnerabilities that exist in the ICT area descend from the lack of awareness by the main players in this infrastructure (information systems and networks end users and administrators, technology developers, product provisioning managers, etc.) of the importance of defining an appropriate approach to ICT security.

The primary consequence of this lack of awareness is the absence of adequate ICT security management processes and procedures. In addition, information and training activities tend to be inadequate to properly train qualified personnel. This scenario in fact hinders the possibility of limiting ICT vulnerabilities to acceptable levels and adopting effective countermeasures.

Therefore, a possible strategy to increase the security of a critical infrastructure could be to launch initiatives that focus on awareness, education and training of all involved parties, such as, for example:

- the promotion of a global program to raise awareness at all levels about the importance of a security policy for ICT systems
- the adoption of education and training programs to support ICT security requirements
- the promotion of security certifications (refer to par. 3.2.2.2.4.1).

We will discuss the above-mentioned initiatives in the following paragraphs.
3.3.3.1 Promotion of awareness raising programs

A limited knowledge and awareness of the existence of a specific security problem that concerns ICT infrastructures, vanishes the effort to search for and adopt possible solutions that, in many cases, are already available on the market.

In other cases, there is no awareness of the importance of making a network element more secure; for example, a company that does not understand that their web server’s identification and authentication system is inadequate, could allow eventual unauthorized users to take control of their server and exploit its resources.

If one System component is not secure, this can have serious consequences for the other components and therefore, any action anyone takes to make his own network portion more secure will contribute to the security of the whole system.

3.3.3.2 Actions taken by other countries

The above-mentioned issues have been addressed by the United States Government in a document that contains, among other things, a set of actions for managing the human factor in the context of ICT security\(^2\).

Table 12 illustrates the Actions and Recommendations set forth in the document.

---

\(^{11}\) On November 25, 2002, President Bush signed the legislative act creating the Department of Homeland Security (DHS). DHS has been given the responsibility to ensure Cyberspace security.
### Promotion of a global national awareness program

DHS, working in coordination with appropriate federal, state, and local entities and private sector organizations, will facilitate a comprehensive awareness campaign including audience-specific awareness materials, expansion of the StaySafeOnline campaign, and development of awards programs for those in industry making significant contributions to security. (A/R 3-1)

DHS, in coordination with the Department of Education, will encourage and support, where appropriate subject to budget considerations, state, local, and private organizations in the development of programs and guidelines for primary and secondary school students in cybersecurity. (A/R 3-2)

Home users and small businesses can help the Nation secure cyberspace by securing their own connections to it. Installing firewall software and updating it regularly, maintaining current antivirus software, and regularly updating operating systems and major applications with security enhancements are actions that individuals and enterprise operators can take to help secure cyberspace. To facilitate such actions, DHS will create a public-private task force of private companies, organizations, and consumer users groups to identify ways that providers of information technology products and services, and other organizations can make it easier for home users and small businesses to secure their systems. (A/R 3-3)

A public-private partnership should continue work in helping to secure the Nation’s cyber infrastructure through participation in, as appropriate and feasible, a technology and R&D gap analysis to provide input into the federal cybersecurity research agenda, coordination on the conduct of associated research, and the development and dissemination of best practices for cybersecurity. (A/R 3-6)

### Adoption of adequate education and training programs at national level

DHS will implement and encourage the establishment of programs to advance the training of cybersecurity professionals in the United States, including coordination with NSF, OPM, and NSA, to identify ways to leverage the existing Cyber Corps Scholarship for Service program as well as the various graduate, postdoctoral, senior researcher, and faculty development fellowship and traineeship programs created by the Cyber Security Research and Development Act, to address these important training and education workforce issues. (A/R 3-7)

DHS, in coordination with other agencies with cybersecurity competences, will develop a coordination mechanism linking federal cybersecurity and computer forensics training programs. (A/R 3-8).

### Promotion of aids to the public and the private sectors for the acceptance of security certifications

Promotion of aids to the public and the private sectors for the acceptance of security certifications. DHS will encourage efforts that are needed to build foundations for the development of security certification programs that will be broadly accepted by the public and private sectors. DHS and other federal agencies can aid these efforts by effectively articulating the needs of the Federal IT security community. (A/R 3-9).

| Table 12: Actions and Recommendations included in the document [5] | }
3.3.3.3 Personal and procedural countermeasures adopted by the Italian National Security Authority (Autorità Nazionale per la Sicurezza - ANS)

Still in the «Human Factor» area, we briefly mention the document [6] that, among the various topics, deals with the issue of security measures, also called countermeasures, which essentially belong to 4 categories:

- Physical measures
- Personal measures
- Procedural measures
- Technical hardware and software measures

Always regarding the human factor, in the “personal measures” and “procedural measures” paragraphs, we find the definition of a series of countermeasures, which, if properly implemented, can significantly reduce the vulnerability level of critical ICT systems. The following is an excerpt of such countermeasures:

**Personal measures**

<table>
<thead>
<tr>
<th>Pe1</th>
<th>Secrecy clearance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pe2</td>
<td>Information access assignment according the need to know</td>
</tr>
<tr>
<td>Pe3</td>
<td>Instructions on security and personnel management</td>
</tr>
<tr>
<td></td>
<td>1. Motivate personnel to follow the policy of the company or institution to which he/she belongs</td>
</tr>
<tr>
<td></td>
<td>2. Train personnel illustrating the possible threats (i.e. password disclosure) and how to limit their effects</td>
</tr>
<tr>
<td></td>
<td>3. Keep the attention high on security regulations using posters, circular letters and educational videos</td>
</tr>
<tr>
<td>Pe4</td>
<td>Personnel training</td>
</tr>
<tr>
<td></td>
<td>1. Department tests to evaluate personnel's level of computer alphabetization</td>
</tr>
<tr>
<td></td>
<td>2. Internal Course, based on test results, on the use of the department's procedures</td>
</tr>
<tr>
<td></td>
<td>3. Final exams to evaluate the acquired knowledge level</td>
</tr>
<tr>
<td>Pe5</td>
<td>Creation of a user support staff that will perform security controls and provide support on security related issues</td>
</tr>
</tbody>
</table>
## Procedural measures

<table>
<thead>
<tr>
<th>Pr1</th>
<th>Data and software back up procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Backup plan</td>
</tr>
<tr>
<td>2.</td>
<td>Rotation of back-up media</td>
</tr>
<tr>
<td>3.</td>
<td>Backup at the end of the day</td>
</tr>
<tr>
<td>4.</td>
<td>Assignment of responsibilities and tasks</td>
</tr>
<tr>
<td>5.</td>
<td>Creation of multiple copies</td>
</tr>
<tr>
<td>6.</td>
<td>Keep documentation of the copies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pr2</th>
<th>...</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Pr3</th>
<th>...</th>
</tr>
</thead>
</table>

| Pr4 | Control of the garbage disposal containers to check if they contain objects (printouts, disks, paper) that can pose a security risk. |

<table>
<thead>
<tr>
<th>Pr5</th>
<th>...</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Pr6</th>
<th>Emergency plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Distribute the Procedures Manual to assigned personnel</td>
</tr>
<tr>
<td>2.</td>
<td>Place emergency procedures summary posters</td>
</tr>
<tr>
<td>3.</td>
<td>Define rules to determine the presence of a real emergency situation</td>
</tr>
<tr>
<td>4.</td>
<td>Define procedures for the recovery of damaged data</td>
</tr>
<tr>
<td>5.</td>
<td>Provide an emergency procedures checklist</td>
</tr>
<tr>
<td>6.</td>
<td>...</td>
</tr>
<tr>
<td>7.</td>
<td>Keep backup storage in fireproof safes</td>
</tr>
<tr>
<td>8.</td>
<td>...</td>
</tr>
</tbody>
</table>
3.3.4 Recommended Contractual framework

In order to complete our overview on the protection of communication networks and after having analyzed the technical and human factors, we have to focus our attention also on the relationships with service providers and in particular on the contractual aspects.

When writing a contract with external companies for the provision of services the unavailability of which, should it exceed an established amount of time, would cause a company to face an emergency/crisis situation, the following aspects, among others, should at least be considered:

1. Check that the provider does not rely on external structures (technological/human resources). If this is not the case, verify whether the processes/procedures that are employed by such structures to guarantee, in case of internal emergency/crisis situations, the continuity of the services they provide to the CII, are coherent with the performance levels defined in the contract. Check whether the provider is taking sole, total responsibility or if he is sharing it with third parties.

2. Verify that the service provider has signed agreements that, in case of emergencies/crises that should involve multiple entities, include support and intervention plans in which service recovery times are differentiated by company and priority. In this case, it would be advisable to include in the contract a recovery priority clause.

3. Make sure you will receive proper documentation (i.e. monthly report) of the provided service levels.

The following is a list of recommendations on the security aspects we think it would be useful to check in contractual frameworks and SLA (Service Level Agreements) with telecommunication services providers.

**Warranties and certifications**

• Assistance in understanding the complexity of the CII’s net-
work and collaboration, according to agreed methods, in finding solutions that guarantee maximum resiliency

- Employment of technically qualified resources in order to guarantee the security of the CII
- Commitment to jointly operate with the CII for service continuity and «disaster recovery» planning, including the planning of tests to verify and guarantee security.
- CII have the responsibility of planning the continuity of their services and of «disaster recovery» planning; many Providers guarantee their assistance in these activities, but their support cannot be covered by network services provision contracts.
- Certification of the complete «separation» and diversity of the services in order to comply with the requirements of the CII.
- Certification on maintaining the resiliency of the «separation» and the diversity over time.

**Contracts and Transparency**

- Include an appropriate transparency grade
- If services «separation» is a primary project requirement, request full visibility of the network infrastructures that are necessary to guarantee end-to-end separation
- Establish appropriate plans for emergency management and ensure that the plans will undergo periodic reviews
- Establish appropriate escalation procedures in order to guarantee that the specific issue will be managed with the level that the importance of the event requires
- Link escape clauses to SLA fulfillment
- Agree on scope and procedures of periodic technical audits.
Availability Measures

• Include service availability, recovery times and other well-defined quality indicators and precise measuring mechanisms

• Clearly determine the responsibilities for availability guarantees.

Threat evaluation

• Evaluate the threats against network infrastructures and specify how the service provider can be involved in the effort to reduce the risks connected with such threats

• Verify the resilience of the network services purchased through subcontracting.

3.3.4.1 Additional suggestions

In addition to what is mentioned in the previous paragraph, we provide some suggestions that represent organizational «Best Practices» in the field of contracts with service providers:

Verify that the services that are provided to the CII can be adapted to new situations that might arise after the signing of the contract

Ensure the provider has adequate emergency plans in case of power failure and that he performs the prescribed periodic checks

Ensure that the network provided to the CII will remain resilient over time

In case of outsourcing contracts that include activities that are particularly sensitive in terms of security and continuity of service, request the Service Provider to submit all the documentation on the provided service levels at least monthly. If the Provider’s services concern critical systems (IT security systems, corporate communication network systems, mission-critical data processing centers, etc.), ensure that your Company will be provided with real-time monitoring tools of
the systems controlled by the outsourcer and that you will anyway receive all log documentation every fifteen days.
This volume has been intended for all the managers of national critical infrastructures, public or private, with the aim of directing greater attention and raising awareness on the possible relationship and interdependences that can exist between critical infrastructures and telecommunication infrastructures.

Electronic communications are a resource that crosses all the infrastructures (critical and not critical) of a nation and play a particularly delicate role both for the normal functions of the different infrastructures and for all the aspects that relate to the management of emergency situations and recovery actions.

In particular, the proliferation of information technologies and the convergence of transmission channels have magnified the strategic role played by telecommunications in terms of the support they provide to the different national infrastructures. These same phenomena have, in addition, contributed to amplify the interdependence level that exists between the various infrastructures.

This new different scenario and the rising threats that are mainly associated to the terrorist risk, have led governments to define strategies to improve the robustness and the security of the system of infrastructures that are at the core of every developed country.
In this context, together with the physical protection of the infrastructures, it is essential to also consider the security aspects related to the information systems that support the great majority of national infrastructures.

This volume has precisely intended to highlight the main elements that have to be considered in the analysis of the vulnerabilities of these information systems and some of the possible countermeasures that can be adopted.

In fact, the growing importance of ICT technologies in terms of the service continuity of the various infrastructures requires us to consider with great attention the security, protection and robustness aspects of the different information systems and of their communication networks (Chapter 1).

This activity must start from the analysis of the vulnerabilities of the system and, in addition to the identification of the assets that need to be protected, we must also carefully consider all the elements of interdependency and the possible threats. These elements represent the starting point for the definition of appropriate security strategies to reduce the risk below a level that is deemed to be compatible with the criticality of the infrastructure under consideration (Chapter 2).

When focusing on the telecommunication networks that support the monitoring and control information systems of the different infrastructures, we must analyze the importance and the strategic value of the information they carry and the characteristics that the underlying network must have.

This analysis leads to classify networks as: maximum-secure networks, secure networks and robust networks. Networks are classified according to their resiliency level and the classes, are characterized by different architectural, topological, procedural and functional elements that ensure the security standards required by the different applications.

A similar focus must be applied to the layers that are above the physical level, where it is necessary to introduce adequate security infrastructures that will guarantee the identification, authentication
and certification of the subjects that operate on the infrastructure and of the information that is being carried over the network. Moreover, the human factor is undoubtedly by far the best resource for the optimal management of anomalous or crisis situations, but, at the same time, not adequately trained and motivated personnel can represent a vulnerability for the entire system. Therefore, it is absolutely necessary to implement adequate information and training processes on the various aspects of security and on international standards and certifications.

In particular, certifications represent a very important element both for the security evaluation of the single products (Common Criteria based certification) and for the projects (BS7799 based certification).

Of course, network security must also take into account, in addition to computer technology aspects, support services and infrastructures and special attention must be devoted to ensure an adequate power supply.

The presence of interdependencies between the different structures requires the joint management of crisis events in order to limit their consequences. At this regard, we can envision the constitution of a specific crisis management unit where all the infrastructures involved can be represented. This crisis unit, comprising adequately trained members who should also be supported by specific methodological and technologic tools, coordinates the necessary initiatives for the management of the different aspects of the crisis.

The included appendices complete this work with the description of the actions that have been taken by an important Italian operator (highlighting the aspects that concern risk analysis and management and also the procedural, methodological and operational resources that must be activated in case of a crisis) and contain also a self-help questionnaire that can be used by operators to perform an auto evaluation of their own level of dependency from telecommunication infrastructures and therefore achieve a clearer awareness of their own vulnerabilities.

The questionnaire covers the contractual elements that are specified in the SLA. Their function is to ensure that provided serv-
ices will meet an agreed, predetermined and verifiable quality level and also to define specific charges in case of breach of contract by the Provider. These guarantees and charges also explicitly and, more often, implicitly depend on procedural actions and technical measures that have to be adopted by the customer. An eventual organizational or technical fault by the customer can lead to disputes concerning the interpretation of the SLA and especially of the clauses concerning damages for alleged infringements of contract by the Provider.

In order to avoid these situations and, most of all, in order to better guarantee that the conditions of the SLA will be met, it is strongly advised to agree with the Service Provider, in explicit and detailed form, the set of conditions that must be met by the Organization in order for the SLA to be considered valid.

These conditions are usually included in a new contractual document called Operation Level Agreement (OLA).

In very general terms, OLA and SLA should be parallel documents where to each contractual prescription that concerns the Provider in the SLA, corresponds the set of prescriptions (OLA) that must be complied with by the Organization in order for the SLA to be applied as both parties desire.

In case of disputes, in the presence of a well-coordinated SLA-OLA pair, there should not be any objection concerning what the procedural and technical obligations/commitments of the Provider and the Customer were, but only about if those particular procedures and technical measures have been implemented.

Two solutions can be adopted to solve this last aspect of the problem.

The first is to have the Provider control the actions undertaken by the customer. This approach, however, might be considered too invasive by the customer or too difficult to be put into practice.

The second solution is to entrust these controls to a trusted third party that is accepted by both the Provider and the customer.
This trusted third party could be a subject that operates within the National Scheme for the Certification of IT Security, may it be an IT Security Evaluation Laboratory or an Assistant.

The importance of the robustness and the resilience of communication infrastructures is the center of a debate that has been launched at European level by the Dutch presidency: the recent events, from the Twin Towers to the tsunami, have demonstrated that prevention is simply not enough and that we must work on the pre-emptive organization of emergency management (also at local level) and on recovery plans.

Italy has a proven experience in emergency management and recovery with many years of exemplary successes (let’s just think about the 2003 power failure, just as an example) and is internationally viewed as a country of reference in this field.

This volume has intended to serve as a starting point to promote an information exchange and the diffusion of Best Practices on the relationships between communication infrastructures and national critical infrastructures.
# Appendix 1 - Acronyms and abbreviations

<table>
<thead>
<tr>
<th>Acron./Abbrev.</th>
<th>Descrizione</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CAO</td>
<td>Certification Authority Operator</td>
</tr>
<tr>
<td>CII</td>
<td>Critical Information Infrastructure</td>
</tr>
<tr>
<td>CIIP</td>
<td>Critical Information Infrastructure Protection</td>
</tr>
<tr>
<td>CMD</td>
<td>Carta Multiservizi della Difesa</td>
</tr>
<tr>
<td>CNI</td>
<td>Critical National Infrastructure</td>
</tr>
<tr>
<td>CNII</td>
<td>Critical National Information Infrastructure</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off The Shelf</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Relationship Management</td>
</tr>
<tr>
<td>CTI</td>
<td>Computer Telephony Integration</td>
</tr>
<tr>
<td>DMZ</td>
<td>DeMilitarized Zone</td>
</tr>
<tr>
<td>D-OCSP</td>
<td>Distributed On Line Certificate Status Protocol</td>
</tr>
<tr>
<td>DOS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DR</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>EAL</td>
<td>Evaluation Assurance Level</td>
</tr>
<tr>
<td>JCM</td>
<td>Joint Crisis Management</td>
</tr>
<tr>
<td>HA</td>
<td>High Availability</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host Intrusion Detection System</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IDSS</td>
<td>Intelligent Decision Support System</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPng</td>
<td>IP next generation</td>
</tr>
<tr>
<td>ITSEC</td>
<td>Information Technology Security Evaluation Criteria</td>
</tr>
<tr>
<td>ITSEM</td>
<td>Information Technology Security Evaluation Methodology</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union – (International organization within the United Nations System that works on the definition of standards for the coordination of global telecom networks and services)</td>
</tr>
<tr>
<td>IVR</td>
<td>Interactive Voice Response</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>MLPP</td>
<td>Multi-Level Precedence and Pre-emption</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NIDS</td>
<td>Network Intrusion Detection System</td>
</tr>
<tr>
<td>OCSI</td>
<td>Italian Security Certification Body for Commercial Information Systems and Products</td>
</tr>
<tr>
<td>OCSP</td>
<td>On Line Certificate Status Protocol</td>
</tr>
<tr>
<td>OHSAS</td>
<td>Occupation Health and Safety Assessment</td>
</tr>
<tr>
<td>OSS</td>
<td>Operations Support System</td>
</tr>
<tr>
<td>OU</td>
<td>Organizational Unit</td>
</tr>
<tr>
<td>NP</td>
<td>Network Port</td>
</tr>
<tr>
<td>CMP</td>
<td>Crisis Management Plan</td>
</tr>
<tr>
<td>JCMP</td>
<td>Joint Crisis Management Plan</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network</td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority</td>
</tr>
<tr>
<td>RTC</td>
<td>Real Time Certification</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Quotation</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>TBD</td>
<td>To Be Defined</td>
</tr>
<tr>
<td>TOE</td>
<td>Target Of Evaluation</td>
</tr>
<tr>
<td>CMU</td>
<td>Crisis Management Unit</td>
</tr>
<tr>
<td>JCMU</td>
<td>Joint Crisis Management Unit</td>
</tr>
<tr>
<td>VR</td>
<td>Virtual Reality</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
Appendix 2
Reference documents


[2] Linee Guida del Governo per lo sviluppo della Società dell’Informazione - Commissione dei Ministri per la Società dell’Informazione - May 2002


Appendix 3
Reference standards and regulations

In preparing this document, we have referred to the following national and international standards and regulations. The following is a non-exhaustive list of standards and regulations.

**ITU-T**


- M.ets (futura M.3350), "TMN service management requirements for information interchange across the TMN X-interface to support provisioning of telecommunication capabilities for disaster relief operations and mitigation", April 2004

- Y.roec (futura Y.1271), "Framework(s) on network requirements and capabilities to support emergency communications over evolving circuit-switched and packet-switched networks", draft H.460.4, "Call priority designation for H.323 calls", November 2002

I.255.3, "Community of interest supplementary services: Multi-level precedence and preemption service (MLPP)", July 1990

Q.735.3, "Stage 3 description for community of interest supplementary services using Signalling System No. 7: Multi-level precedence and pre-emption", March 1993

Q.955.3, "Stage 3 description for community of interest supplementary services using DSS 1: Multi-level precedence and preemption (MLPP)", March 1993


Q.2764 (1999) Amendment 1, "Support for the International
Emergency Preference Scheme", 12/2002


ETSI

- TR 101 300, "Telecommunications and Internet Protocol Harmonisation Over Networks (TIPHON)", v.2.1.1, October 1999

NSTAC


- White Paper, "The Emergency telecommunications Service (ETS) in Evolving Networks", v.3.0, 4 February 2002

IETF


- RFC 3523, "Internet Emergency Preparedness (IEPREP) Telephony Topology Terminology", Polk, April 2003

- RFC 3690, "IP Telephony Requirements for Emergency Telecommunication Service (ETS)", Carlberg-Atkinson, February 2004

- RFC 3689, "General Requirements for Emergency Telecommunication Service (ETS)", Carlberg-Atkinson, February 2004


INTERNET DRAFT draft-polk-reason-header-for-preemption-00.txt, "Extending the Session Initiation Protocol Reason Header to account for Preemption Events", Polk, 8 October 2003

RFC 3326, "The Reason Header Field for the Session Initiation Protocol (SIP)", Schulzrinne-Oran-Camarillo, December 2002

INTERNET DRAFT Draft-pierce-tsvwg-pref-treat-examples-00.txt, "Examples for Provision of Preferential Treatment in Voice over IP", Pierce-Choi, April 2004

INTERNET DRAFT Draft-pierce-tsvwg-assured-service-req-00.txt, "Requirements for Assured Service Capabilities in Voice over IP", Pierce-Choi, April 2004


INTERNET DRAFT Draft-silverman-tsvwg-mlefphb-01.txt, "Multi-Level Expedited Forwarding Per Hop Behaviour (MLEF PHB)", Pierce-Choi, 1 October 2004

INTERNET DRAFT Draft-baker-tsvwg-mlpp-that-works-02.txt, "Implementing MLPP for Voice and Video in the Internet Protocol Suite", Baker-Polk, 2 October 2004

INTERNET DRAFT Draft-baker-tsvwg-mlef-concerns-
02.txt, "MLEF without Capacity Admission Does not Satisfy MLPP Requirements", Baker-Polk, 5 October 2004

ISO

- ISO 17799, "Information Security (INFOSEC)"

AND SYSTEM/PRODUCTS CERTIFICATION

NIST e ISO

- Draft SP 800-70 The NIST Security Configuration Checklists Program
- SP 800-64 NIST Security Considerations in the Information System Development Life Cycle, October 2003
- SP 800-63 NIST Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, June 2004
- SP 800-61 NIST Computer Security Incident Handling Guide, January 2004
- SP 800-60 NIST Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004
- SP 800-59 NIST Guideline for Identifying an Information System as a National Security System, August 2003
- SP 800-50 NIST Building an Information Technology Security Awareness and Training Program, October 2003
- SP 800-46 NIST Security for Telecommuting and Broadband Communications, September 2002
- SP 800-42 Guideline on Network Security Testing, October 2003
- SP 800-41 Guidelines on Firewalls and Firewall Policy, January 2002
- SP 800-40 Procedures for Handling Security Patches, September 2002
- SP 800-36 Guide to Selecting Information Security Products, October 2003
- SP 800-35 Guide to Information Technology Security
Services, October 2003
- SP 800-34 Contingency Planning Guide for Information Technology Systems, June 2002
- SP 800-33 Underlying Technical Models for Information Technology Security, December 2001
- SP 800-31 Intrusion Detection Systems (IDS), November 2001
- SP 800-23 Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, August 2000
- SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
- SP 800-12 An Introduction to Computer Security: The NIST Handbook, October 1995
- INCITS/ISO/IEC TR 13335 Information technology - Guidelines for the management of IT Security
  Part 1: Concepts and models for IT Security
  Part 2: Managing and planning IT Security
Part 3: Techniques for the management of IT Security
Part 4: Selection of safeguards
Part 5: Management guidance on network security

- 2. BS7799-2 - Information security management systems - Specification with guidance for use.
- 4. ISO/IEC TR 13335-2, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 2: Managing and planning IT security
- 5. ISO/IEC TR 13335-3, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 3: Techniques for the management of IT security
- 6. ISO/IEC TR 13335-4, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 4: Selection of safeguards
INTRODUCTION

Over the last years Terna, the company who owns the Italian National Transmission Grid (NTG), has developed a sound experience in the field of risk management and has obtained significant results in the achievement of the corporate objectives of quality of service and operational excellence.

The present document illustrates the main elements that characterize one of the main Business Continuity processes employed by the company: the application of risk analysis to the strategic functions of operation and monitoring of the electrical systems of the NTG.

The following is a concise description of the method that has been used for risk identification and assessment and of the action plan that applies to the most critical cases, in terms of the security of the national electrical system, to reduce the level of risk of any situation to a sustainable level through the analysis and the evaluation, starting from operating experiences, of an extensive list of potential external threats and internal vulnerabilities.

The document also describes the control cycle, a crucial element of operational risk management that is dedicated to the systematic assessment of the actual implementation of prevention/mitigation actions, of the existence of an effective Disaster Recovery system.
and also of the appropriate definition of the organization that supports the process at all levels.

This is one of Terna’s primary Business Continuity processes because it applies to the continuous surveillance of operations and of the NTG, the activities for the control and the implementation of service restore in case of power failures and the organizational structures that are necessary for ordinary operation and crisis situations.

**TERNA’A ASSETS - CNI/CII**

Terna owns over than 90% of the national electricity transmission grid, about 300 stations, 566 transformers and over 38,600 km of 380/220/130 kV power lines. Terna’s infrastructure covers the entire national territory (A4.1) and is dedicated to the distribution of high and very high voltage electricity from production plants and from foreign links for imported electricity, to the supplying points of a several large customers (high voltage consumers) and generally of the various distribution companies that deliver the electricity to homes, factories and other users.

Terna has the responsibility of the effective and efficient management of the grid, in accordance with the procedures established by the National Transmission Grid Operator (Gestore della Rete di Trasmissione Nazionale – GRTN). With primary objectives such as security and quality of service (availability of the network elements, continuity and recovery capability) and the reduction of unavailability times and costs, Terna’s operations and network configuration monitoring and real-time control are conducted through three remote operation centers (Tele-management Centers) and Terna also carries out ordinary and extraordinary maintenance operations and also grid development initiatives established by NTGO (due to functional requirements, rationalizations, modifications or regulatory duties) through its territorial organization.
Fig. A4.1: Terna's CNI
Among its assigned duties, Terna has the duty to maintain operational relationships also with, in addition to the National Transmission Grid Operator, the other production and distribution companies of the national electrical system, Third Parties, Authorities and Institutions (Prefects, National Forest Police, the Civil Protection National Service).

The following is a list of some of the definitions that are contained in the document.

**Blackout**

Total absence of voltage in systems or part of the electrical network due to service disruptions that, because of their duration and/or extension, can cause extensive and relevant power outages.

**Business Continuity**

Process that is aimed at ensuring the prevention and the effective management of critical events through prevention systems, organizational structures, operational rules and reciprocally coherent tools/means. The process is articulated in the following four macro phases:

- **Preventive phase**: risk analysis and evaluation, design and implementation of prevention systems, of the operational event management plan (emergency plan and Disaster Recovery plan) and personnel training.
- **Management phase**: governance of critical events, damage containment and return to normal operation.
- **Follow up phase**: assessment of the effectiveness and update of prevention and recovery systems - ex-post evaluation of critical events management actions and implementation of improvement actions according to the «continuous improvement» model.

**Crisis**

Damaging event that has an exceptional impact on the company and that usually has a very significant impact on public opinion. The state of crisis requires extraordinary management measures (i.e. Crisis Committee).
| **Damage** | Adverse impact caused by an event, quantifiable in economic terms |
| **Disaster Recovery (DR)** | The complex of organizational, technological and logistic interventions that allow to restore the continuity of the company’s processes and infrastructures that have become inoperative or inaccessible due to critical events |
| **Emergency** | Damaging event that diverts the course of enterprise activities and that can be prevented and/or managed by specific plans (emergency plans). The plant operation and monitoring process considers two emergency levels «Normal alarm condition» and «Disturbed condition» |
| **Critical event** | Any incident or situation that occurs in a given place and time and that might determine emergency and/or crisis conditions |
| **Impact** | Consequence of the occurrence of an event. It can generate both positive and negative effects for the enterprise. It can be expressed both in qualitative and in quantitative terms |
| **Assumptions** | Basic assumptions about possible disaster situations caused by different types of phenomena for which the recovery plan must be developed. There are two types of assumptions: |
| | - frequency based (expected probability, Pareto diagram) |
| | - worst case condition based (attacks, etc.). |
| **Risk exposition level** | Value obtained through the correlation between the probability of the event and the value of the damage caused by the event |
| **Threat** | Particular event or situation, usually external to the company’s organization, that could cause a negative impact |
| **Probability** | Frequency of the occurrence of an event, meas- |
ured over a sufficient period of time with respect to the process

Unit of risk
A system part potentially subject to damaging events

Vulnerability
Element, generally inside the enterprise perimeter, which elevates the risk profile and causes an increase of the probability and/or of the impact

THE CONTEXT OF APPLICATION OF RISK MANAGEMENT

The functions of real-time grid assets operation and monitoring are deployed by highly specialized technical personnel with the support of a complex integrated technological system of ICT components, of different types and functions (data acquisition nodes, communication networks, control centers, SCADA servers, dedicated Databases and software, grid management applications, etc.) distributed across the entire national territory.

As shown in Fig. A4.2, this process is based on the combination of activities (organization and resources, with key factors such as professional skills, training, recruitment, procedures, etc.) and technologies (with key factors such as innovation, architectures, standards, diversifications, etc.).

This logical and physical infrastructure can be considered as the «nucleus» of Terna’s CII for its crucial role in the management of the electricity system, in fact it:

• manages information flows from/to power stations and guarantees their integrity and security

• provides operators with a real time representation of the state of the electrical system (grid topology, signals and measures)

• supports all the actions for the remote management and control of power equipment
guarantees the communications tools for emergency activity.

The infrastructure uses Fig. A4.3 specific distributed components to interface with power plants and it also employs several dedicated ICT components, such as processing systems, HMI, Databases, ad hoc telecommunication networks that include both geographical data transmission platforms (so called SCTI-NET made up with nodes, routers, supervision systems, protection systems) and telephone systems that are specifically optimized to provide an adequate support to National Transmission Grid operations activities.

The National Electricity Transmission Grid must be maintained in optimal working conditions (or status) through operation and monitoring activities: the global process is a coordinated complex of organi-
zational, functional, operational and project activities that are designed to optimize operations management, where the close interaction between the organization and support technologies plays a crucial role.

fig. A4.3 - Functional blocks representation of the CII
THE PHASES OF THE CII RISK MANAGEMENT PROCESS

In consideration of the above, risk management for the control and communication infrastructure is an entirely separate process, dedicated to the engineering, the innovation and the maintenance of the CII, and it is extremely critical because the activities performed by the corresponding technological components are very important for the security of the electrical grid (especially under disturbed conditions).

The CII’s risk management process has been developed according to the double cycle hierarchical scheme that is normally used in Terna - Global and Operational - PDCA (Plan, Do, Check, Act).

Three risk categories have been defined and analyzed for the CII: functional risk (concerning service continuity), physical risk (concerning asset availability and integrity) and logical-informatics risk (concerning software and data security).
The first phase of the process consisted in an in-depth analysis of the elementary functions of the infrastructural system and of the impact that potential critical events could have on their operation in order to identify possible project (prevention systems), operational, maintenance solutions to minimize the effects of the events.

The final objective of this phase is to provide the company’s management with a complete picture of the criticalities that can condition the functioning of a primary operating process and with a list of possible alternatives that could guarantee better security conditions, always, of course, taking into account financial considerations and after having evaluated with great attention the grade of dependency of the company’s objectives and the corresponding damage that could derive from a persistent unavailability of that particular process. A top-down approach, structured according the following scheme, was used to achieve this objective:

I. risk scenarios analysis (natural disasters, malicious acts, extensive failures, etc.)

II. process modeling and identification of critical events (threats and vulnerabilities)

III. risk evaluation through impact-analysis and probability of occurrence techniques of the consequences on the primary process, taking into account possible threat/disturbance phenomena and their effect on the functions and the performances of the process

IV. identification and design of mitigation/correction actions: choice of the technical actions that allow to reduce the influence of the considered factors within acceptable levels;

V. development, implementation and review of mitigation/correction actions and of backup structures

VI. definition and execution of the executive plans for the implementation of mitigation/correction actions in order to respond to the occurrence of foreseen critical events (threats, vulnerabilities) with pre-established methods and emergency/crisis organization (Disaster Recovery) monitoring of the entire process and structuring of controls.
Practically, a graphic realization was produced, where the CII was broken down into elementary sections that could be subject to possible critical events and/or could propagate an anomaly (Fig. A4.4).

Starting from the representation map of the elementary components, a search was conducted to identify any potentially adverse event/scenario that could pose as a threat/vulnerability to the physical and human capital of the company and/or for its organizational, man-
agement and financial capabilities.

This phase, which represents the most critical moment of the entire analysis process and will inevitably influence the quality of the results, has been performed using the problem solving method (i.e. cause/effect diagram), starting from the identification of the critical events/scenarios and their association to the risk unit and arriving to the identification of the cause that generates the event/scenario and of its effects on the process.

Fig. A4.5 offers a schematic representation of the result of the sequential breakdown into increasingly elementary functional systems, in order to more easily identify and isolate the parts that may be subject to potentially damaging events.

The critical events that have been identified have been classified under «threats» and «vulnerabilities» according to their external and internal origin and their most significant causes and characteristics have been described.

The greater the accuracy and the quality of the identification of the events, the more satisfactory the results will be: in this phase it is important to not leave any possible option unexplored, because an unidentified risk event can leave the organization without any defense and it is also important to correctly evaluate the impact of an event, to avoid, for example, idle expenses.

The identification of the vulnerabilities requires very accurate analyses and specialized technical skills: for each identified critical event/adverse scenario, an estimate of the probability of occurrence has to be produced using every available information element, indicating its origin, the sources and the criteria that have been used (historical data, reliability analysis, project data, etc.). In addition, also the potential consequences of the event have to be evaluated, in particular the event’s direct/indirect/consequential effects on the different elements of the process that are involved, without considering, in this phase, the effects of eventual defense systems that might have been already implemented.

Whenever possible, the damage/impact caused by the event on the company’s performance must be quantified in economic terms.
Fig. A4.5 - Cause-effect diagram (Ishikawa) of management system
because the evaluations/decisions of the company are of course subject to financial constraints; a series of assumptions have been made to estimate the economical damage, including the consequences in case of failure to comply with NTG operating duties, internal costs, damages caused to third parties.

The critical events/scenarios that have to be covered by prevention systems have been identified according to the «Level of exposure to the potential risk», measured through the comparison with an acceptability curve (generically represented in Fig. A4.6), then mapped in a Matrix (following table), where the exposure level is the result, conventionally, of the combination between the «probability of the event» in a reasonable observation period and the value of the «damage», within opportune identified probability and damage ranges that are coherent with the objectives and the strategies of the company.

In the case of the process under analysis, the introduction of prevention systems has been defined as absolutely necessary in case of an «extreme» or «very high» level of risk exposure, while in the cases of «high» or «medium» levels, it has been decided to evaluate, case by case, using a costs/benefits analysis, the way in which the risk could be accepted, reduced or transferred elsewhere.
After having identified the prevention systems that are necessary to limit the criticality of the events/scenarios that are considered critical, the criticalities of the events/scenarios have been assessed taking into account the previously identified prevention systems (according to the scheme of the following table): if a reduction of the criticality to acceptable levels is identified, then the systems will become part of a plan of improvement actions, with corresponding priorities.

This phase has been conducted taking into account operational experience (occurred events), hypothetical scenarios, the evolution of the market of ICT control systems and an in-depth financial analysis (financial evaluation of security and of risk cost, selection of

![Risk Level Table]

<table>
<thead>
<tr>
<th>Probability value</th>
<th>Damage value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NULL (&lt; 0,1)</td>
<td>LOW 1 MEDIUM 2 HIGH 3 VERY HIGH 4 EXTREME 5</td>
</tr>
<tr>
<td>LOW (0,1-0,4)</td>
<td>LOW 1 MEDIUM 2 MEDIUM 3 MEDIUM 3 VERY HIGH 4</td>
</tr>
<tr>
<td>MEDIUM (0,4-0,7)</td>
<td>MEDIUM 2 HIGH 3 VERY HIGH 4 stay EXTREME 5</td>
</tr>
<tr>
<td>HIGH (&gt;0,7)</td>
<td>MEDIUM 2 HIGH 3 VERY HIGH 4 EXTREME 5 EXTREME 5</td>
</tr>
</tbody>
</table>
the security grade, cost/benefits ratio of alternative choices).

The design of the Business Continuity system has defined with extreme accuracy procedural steps and actions, the professional figures that have to be involved in the various activities, hardware and software resources and all the elements that are required to translate the coordinated complex of all the actions for the modification or integration of the prevention systems into technical terms.

The evaluations have mainly concerned systems, components and networks reliability levels, the stability of IT systems, the certification of the modules, the introduction of redundancies sufficient to sustain multiple failures (i.e. hot stand-by SCADA systems, dual processor RTUs, dislocation of resources in diversified sites, redundant communication routes and on alternative physical links), the enhancement of the CII supervision activity, the use of adequately skilled professional resources and the adequacy of the logic-informatics risk prevention systems.

The feasibility requirements and the operational programs of the prevention systems have been defined in an Action plan, in accordance with corporate objectives and responsibilities and the fulfillment of procedural obligations (from the procurement of resources, to the training of involved personnel, the preparation of check lists of the controls that have to be performed to guarantee that the Business Continuity System will work well, etc).

At the end of a homogeneous design and implementation phase and also in the light of unexpected events or new opportunities provided by innovations or any other new phenomenon that can have an impact on the process, it is then necessary to perform periodic feedback analyses of the process that will lead to the assessment of the effectiveness of the prevention systems or to the eventual introduction of corrective elements.
THE DISASTER RECOVERY (DR) SYSTEM AND THE EMERGENCY PLAN

The purpose of a Disaster Recovery system is to restore (and/or maintain) the functions of a particularly critical enterprise process within a limited timeframe and with an emergency/crisis organization that reacts to critical events (threats, vulnerabilities) through the methodical execution of the mitigation/correction actions that have been identified and implemented in the prevention systems development plan (BC system).

It is essentially an organizational instrument that allows managing the period that elapses between the declaration of the state of emergency/crisis and the resume of normal conditions.

In Terna’s case, starting from the initiatives that are described in the Business Continuity plan, a series of procedures have been codified to respond, at the operational level, to any condition or scenario and they correspond to the Disaster Recovery System (DR) of the primary operation and monitoring process of the RTU system.

The DR system uses the prevention systems that have been implemented according to the Business Continuity plan and operates through a plan and an emergency organization that is dedicated to the management of the single emergency and/or crisis situation.

The plan contains specific dispositions, both technical and procedural, that are made known to interested personnel through targeted initiatives and requires the adoption of professional figures, communication flows, equipment and technologies (such as, for example, emergency rooms equipped for the management of the phases of the crisis) that are all specifically dedicated to handle any exceptional situation that should involve the CII.

The following elements concur to the definition of the plan:

• identification of the internal/external sub-systems that participate in the DR system

• identification of the sub-systems that, in case of failure, need to be supported by back-up systems
• determination of the minimum number of persons necessary to ensure the provision of services during emergency situations

• definition of alarm escalation rules for the declaration of the state of emergency and all the levels of the people involved up to top management

• definition of on-call requirements for the persons that are involved in the recovery plan

• preparation of the diagram of activities and times to manage the shifts at emergency sites.

The possible occurrence of a disastrous event that could disrupt normal operating conditions requires the presence of a specific organization that will have the necessary authority and competence to deal with the complex issues connected with an exceptional situation: taking obviously into account the organizational structure that is assigned to oversee enterprise security, it is necessary to outline a hierarchical design that will be functional for the emergency and therefore to identify the bodies that shall declare the state of crisis and operate in case of a disastrous event (partial or total power failures in the national grid, simultaneous failure of multiple control centres caused by external threats and/or internal vulnerability) and define their responsibilities and authority. In the course of an emergency/crisis, all relational, communications and coordination actions must be carried out in an orderly, timely and appropriate manner from the onset of the event.

**ACTIVITIES, ROLES AND TASKS**

- **COMMUNICATION/TRAINING PLAN**

All the actions that concern BC and DR must be known and acquired by all involved subjects: therefore, there is the need to develop and implement a series of targeted training plans, a continuous and effective training program that will ensure a continuing professional update both in the technological field and in the area of the development of behavioral skills. The main goals of training personnel on risk
management and on the execution of emergency plans are:

- generate awareness of the treats that could derive from internal and external changes; i.e. the new opportunities offered by technological advancements could introduce new risks that have to be recognized taken and managed consciously

- provide understanding of the behaviors and of the corresponding operational responsibilities required for the operation of the CNI both in the normal state of the process and in the scenarios covered by the technical-operational risk management

- illustrate the processes that have to be activated in case of anomalies/failures of the main components/systems/infrastructures that support the process or, in any case, in occasion of events that could have potentially disastrous impacts

- illustrate the best methods for monitoring and maintaining the systems that are involved in BC and DR.

In any case, training must be administered every time the technical/operational risk management procedures/instructions are updated and every time new personnel are hired in the Units involved in BC and DR Systems.

Roles and tasks, update cycles, specific action programs (audits, trials and system tests, etc.), operational flow-charts, periodic checks and the corresponding check-lists and improvement actions are all detailed in specific documents of confidential nature that, in some cases, are subject to a restricted circulation within the company.

MAINTENANCE AND EVOLUTION OF BUSINESS CONTINUITY AND DISASTER RECOVERY SYSTEMS

Factors such as the technological evolution of software and hardware systems, especially in the field of process control technologies, the organizational and logistic evolution of the company, the attention drop of the people involved, staff turnover in key roles, can
lead to a rapid obsolesce of the BC and DR systems and therefore they must be periodically reviewed and revised.

Periodic assessments must be conducted to maintain the BC and DR systems in efficient technical/operating conditions and to determine the presence of possible risk factors that have not been previously included in the risk management process.

In Terna, these monitoring actions include cyclical tests, the extraction from information systems of every event that has an impact on the continuity of the plant operation and monitoring process, audits and constant monitoring of the innovations offered by the market.
Appendix 5

Self Assessment questionnaire on the minimum network security requirements

The present Self Assessment questionnaire focuses on the security aspects that are directly connected with telecommunication infrastructures and its purpose is to facilitate the development of network systems and architectures that will possess intrinsic reliability and security characteristics that will allow the Organization, for which this questionnaire is intended, to respond to accidental and/or intentional internal or external events.

An Organization could use different Providers for different services, but it could also ask the provision of same service to multiple Providers in order to guarantee the availability of its critical systems in case of service disruptions. In this case, the questionnaire can also be used to help determine how the different Providers shall cooperate in order to minimize and reduce risks.

The present questionnaire is intended as a support to help assess the requirements of the communication infrastructure of an Organization and does not pretend to be exhaustive.

For a more in-depth review of specific topics that are related to IT Security, please refer to the regulations of the Ministry for Innovation and Technologies.
A - Infrastructures

The present section offers some considerations on the telecommunication infrastructures used by the organization, in consideration of the fact that operational continuity typically depends on the availability of these infrastructures.

A1 Do you have a complete description of the telecommunication infrastructures that are critical for your activity?

A2 Can you classify your telecommunication infrastructures by their grade of importance and/or criticality between high/vital; medium; low?

A3 Can you identify the critical systems that support your telecommunication infrastructures?

A4 Do you have a periodic update plan for the critical systems that support your telecommunication infrastructures?

A5 Can you univocally identify the different parts of the telecommunication infrastructure that is being used to support your critical systems?

It should be possible to univocally identify every system, circuit or trunk part, for example, by using a code formed by a short acronym and/or by a reference number.

A6 Does your Organization share the same above-mentioned identification system with your Provider?

In case an urgent action on the telecommunication systems should become necessary, it is important that you both use the same naming conventions.

B - Network routing

The present section offers considerations on how your critical systems are connected to the communication network.

B1 Are you aware of where in the Provider’s core network your network services connect
Appendix 5

B2 Are you aware of physical routings your network services follow outside your offices?

The last-mile connectivity between your premises and the outer edge of your Provider’s network is often the most difficult link to provide resilience for, for example when the communication services offered by the Provider end at the telephone exchange and he has no control on the services that are provided in the segment that goes from the exchange to the end user.

B3 you are using dual Providers, are you confident that there are no physical routings or points of failure common to both Providers?

C - Dependency

This section is intended to provoke consideration of other components within both your and the Provider’s core network that are vital to the supply of your services.

C1 Within your own premises, do you have visibility of your telecommunications services all the way into the Provider's duct?

C2 Are any parts of the cabling, for example, exposed to external contractors or others beyond your control?

C3 Are there any third party components, such as ADSL Routers, which may fall between areas of responsibility?

C4 Who has responsibility for the safety of the areas identified in C2?

D - Diversity

This section is intended to provoke consideration of single points of failure, whereby loss of a single (network) component will affect multiple critical services.

D1 Do all of your services leave your premises in the same cable?

D2 Are they all in the same duct?
D3 Do your multiple Providers share a duct system?

Consideration should also be given to whether different premises belonging to your organisation are connected to common points within the Provider’s network.

E - Separation

This section is intended to provoke consideration of how different critical services are routed outside of your premises and through the Provider’s network.

E1 Do you know if critical services are routed via different network components so that a failure of one component will not affect all critical services?

E2 Have you specifically asked for this service?

F - New Services

It should not be assumed that dual-Provider is a guarantee of separation. It is common practice within the Telecommunications industry for local access circuits (between the core network and customer premises) to be provided by a third party (TELECOM ITALIA, for example). In this case, it is possible that circuits supplied by different Providers have a common routing.

F1 When you order new services, do you discuss your existing services to ensure there are no dangerous assumptions made about separacy or diversity?

F2 Do you review existing requirements to prevent duplication or compromise?

G - Changes to Network Structure

This section is intended to provoke consideration of how your Providers manage changes to their network infrastructure. It should
not be assumed that a Providers network is static. Changes are continu-
ually taking place, whether temporary (due to planned engineering
work) or permanent (network restructuring including the introduction
of new network components and the removal of old ones). Over time,
services that were diverse or separate could be compromised by these
changes, although it should be noted that Providers would normally
track these changes to ensure diversity/separacy where contracted to
do so.

G1 Do you regularly review your specific resilience requirements with your
Provider?

G2 Do you receive notification from your Provider regarding network:
updates, proposed engineering downtime or other changes to the status
quo?

H - Power

Loss of power at a site, whether at your premises or within the
Provider’s network, is a significant threat to the continuity of the
telecommunications service.

H1 Do you provide standby power on your own premises?

H2 Do you test it regularly?

H3 Do you have visibility of your Provider’s emergency power
provision and the consequences of a power failure on your
Services?

I - Contact in a Crisis

This section is intended to provoke consideration of how you
will contact your service Provider(s) in the event of a catastrophic
impact to the telecommunications network.

I1 Do you have primary and alternate methods for contacting your Provider
(e.g. telephone, e-mail?).

I2 Have you provided your Provider with alternative contact details for your
own response teams?

I3 Have you discussed your respective emergency plans with
your Provider?

I4  What regular updates would you expect your Provider to provide, in the event of such an incident occurring?
I5  Have you asked for this? Is it covered in your SLA or contract?
I6  Have you explicitly reviewed this topic with the Provider? Have these aspects been considered in the contract or in the SLA?

L - IT Security

The present section offers some considerations on IT security aspects in order to include this topic in the issues that concern Critical Infrastructures. The following points focus on the general issues we consider to be the most important:

L1  Is there a registry containing the inventory of all hardware/software?
L2  Are data backups performed with sufficient frequency to guarantee a rapid and full recovery of the system?
L3  Is there a procedural plan to guarantee data availability and integrity?
L4  Do you have operational and periodic procedures to test data recovery to ensure it will work properly in case of threats and/or data loss?
L5  Are your ICT infrastructures redundant enough to ensure operational continuity?