Project no.:	IST-FP6-STREP - 027513
Project full title:	Critical Utility InfrastructurAL Resilience
Project Acronym:	CRUTIAL
Start date of the project:	01/01/2006 Duration: 36 months

Deliverable no.: D12

Title of the deliverable: Dissemination actions and collected publications

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)

Contractual Date of Delivery to the CEC:	31/12/2007
Actual Date of Delivery to the CEC:	18/01/2008
Organisation name of lead contractor for this deliverable	CNR-ISTI

Author(s): Felicita Di Giandomenico[3] (Editor); Geert Deconinck[5]; Susanna Donatelli[6]; Giovanna Dondossola[1]; Mohamed Kaậniche[4]; Paulo Verissimo[2]

Participant(s): (1) CESI-R; (2) FCUL; (3) CNR-ISTI; (4) LAAS-CNRS; (5) KUL; (6) CNIT

Work package contributing to the deliverable:	WP6
Nature:	R
Dissemination level:	PU
Version:	V2
Total number of pages:	30

Abstract:

This deliverable describes the dissemination actions undertaken by the CRUTIAL consortium in WP6. The document is largely based on the Deliverable D5 on dissemination produced at the end of the first year. It partly reorganizes D5 by separating the dissemination channels from the dissemination actions performed during the first year, and then extends the content by including dissemination actions related to the second year. The document also collects the list of publications produced so far and synthetic plans for exploitation.

Given the very high interest of different stakeholders involved in the topics addressed by CRUTIAL, and of the wider community from public authorities to European citizens which need to rely on resilient electricity supply system, dissemination is considered a prominent activity of the project. The results achieved during the project will help in designing and assessing resilient electric power and dedicated information infrastructures that will enable to reduce the frequency, duration and extent of blackouts, and possible cyber threats, by better mastering the various dimensions of interdependencies. This will clearly have a large social and economic impact.

Keyword list: Dissemination, Publications

DOCUMENT HISTORY

Date	Version	Status	Comments
19/12/07	0.0	Internal	First complete draft incorporating the partners contributions – circulated by ISTI-CNR to all the partners
11/01/08	1.0	Internal	Consolidated draft version including all the partners contributions and comments.
17/01/08	V2	Approved	Approved final version.

Table of Contents

1 INTRODUCTION

The project focuses on the electrical power infrastructure and the information infrastructures, by considering different topology realms and different kinds of risks: distinguishing the backbone from the specific information networks and from the infrastructures dedicated to the control and monitoring of the electric power infrastructure, as they usually have different levels of protection; distinguishing faults of different kinds and severities, such as electric power outages and cyber attacks.

The main objective of the project is the investigation of models and architectures that cope with the scenario of openness, heterogeneity and evolvability endured by electrical utilities infrastructures, in the present and near future. The approach taken should support the analysis and management of interdependencies and of the resulting overall operational risk.

Firstly, the project aims to develop comprehensive modelling approaches, supported by measurement based experiments, to analyze critical scenarios in which internal or external faults in a segment of the information infrastructure provoke a serious impact on the controlled electric power infrastructure. The goal is to understand and master such interdependencies to avoid escalating and cascading failures that result in outages and blackouts. The focus is on the modelling and analysis of interdependencies, especially considering various types of failures that can occur in the presence of accidental and malicious faults affecting the information and electric power infrastructures.

Given the complexity of the analysis task, a difficulty is to find the right abstractions of the models. The aim is therefore to produce, from conceptual analysis, generic models that can be refined and instantiated. It is planned to substantiate the abstractions by examples taken from the electric application domain. Another expected difficulty is the heterogeneity of the models, given the very different nature of the various components under study.

Secondly, the project intends to investigate distributed architectures dedicated to the control and management of the power grid, in the perspective of improving the capability of analyzing critical scenarios and designing dependable interconnected power control systems. The architectures under study addresses requirements coming from the needs of flexible electric power services, characterized by dispersed energy resources, on-demand control and generation-load variation from the market.

In consequence, the project's objective is to devise *new architectural configurations* that address the increase in operational risk derived from the analysis made above. This risk derives not only from accidental faults or wrong manoeuvres, but also, and very importantly, from both the degree of vulnerability and the level of threat to which the infrastructures and services are subjected. The objective of preventing escalating failures on the various information infrastructures (monitoring, control, management) that interact on a decentralized power grid can only be met by the combined use of fault prevention and tolerance, and by the simultaneous addressing of accidental and malicious faults, also called intrusion-tolerance, enhanced by the provision of on-line monitoring support to evaluate possible alternative architectural configurations in uncertain and evolving scenarios.

If successful, the advanced solutions devised by CRUTIAL will constitute an important asset in the European technical arena, to be used by electrical utilities R&D, planning, and technology interface departments, to stimulate what we foresee as a dramatic improvement in the overall quality and resilience of electrical utilities infrastructures. Our foresight is that the take-up of these solutions will happen in coordination of the above-mentioned departments, with the several suppliers and providers involved: SCADA suppliers; information systems integrators; intranet/extranet/Internet service and infrastructure providers. The studies performed during the first year, and the preliminary results obtained so far, are promising towards reaching the expected advancements.

The structure of this deliverable is as follows. Section 2 recalls the CRUTIAL objectives and discusses their relevance to the many different stakeholders in the electrical energy sector. The dissemination actions and means adopted by the CRUTIAL consortium are presented in Section 3. Liaisons with related projects and programs are described in Section 4. The specific dissemination effort undertaken during the first year is reported in Section 5, where also the collection of publications relative to the first year is included (distinguished in publications explicitly acknowledging the support of CRUTIAL and those related but without acknowledgement). The specific dissemination effort undertaken during the second year is reported in Section 6, where also the collection of publications relative to the second year is included. Plans for the exploitation strategy are briefly indicated in Section 7. Conclusions and short indication of future dissemination and exploitation plans are drawn in Section 8.

2 RELEVANCE OF CRUTIAL'S OBJECTIVES

Electrical energy is a *crucial* cornerstone of the European society. The *CRUTIAL* project deals with the vulnerabilities related to the trend where Electric Power Systems and Information Infrastructures are becoming more closely intertwined. By modelling the involved interdependencies and developing architectural solutions for a more resilient system, it is crystal-clear that this project will have a strong influence on the architecture of future power transmission and distribution grids, that will allow to deal adequately with the trend towards the diversification of the power generation and power consumption into smaller units *(dispersed generation)*. As a result of the CRUTIAL, one will have architectures that are *provably resilient*, supporting *survivability* of the service under a set of defined circumstances.

By introducing information infrastructure on a logical level on top of the electric power grid, one will be able to fully exploit these infrastructures for both dealing with timely gathering of information and consequently driving efficient countermeasures in case of disturbances (some of which may be fully or semi-automatic), as well as with business control systems for efficient day-by-day provision and usage of power energy. This is in-line with the introduction of commercial Intelligent Electronic Devices, deployed for the protection of citizens against failures (including cyber threats), and for supporting electric power management and control systems.

However, the introduction of such additional levels of information infrastructure will introduce a mutual interdependence between them and the electric power grid. Faults in such additional infrastructural levels may cause errors that propagate to a different level and/or interrupt part of the electric services. As electrical energy is a crucial cornerstone of the European society, it is important that potential faults and the resulting interdependencies are identified, studied, modelled and assessed in detail. CRUTIAL is centred around this better understanding.

Resilience has to be designed with respect to the logical level infrastructure and in connection to the interdependencies between it and the power grid. Also in this field there is heterogeneity of used techniques, based on special redundant power components at the power grid level and on different mechanisms at the logical level. What is not reported yet is a methodical in-depth study on such problems. CRUTIAL is devoted to modelling interdependent infrastructures taking into account multiple dimensions of interdependencies, in order to be representative. Furthermore, the definition of resilient architectural patterns of the dedicated information infrastructure must be based on the analysis and modelling of such interdependent infrastructures.

The results achieved during the project will help in designing and assessing resilient electric power and dedicated information infrastructures that will enable to reduce the frequency, duration and extent blackouts, and possible cyber threats by better mastering the various dimensions of interdependencies. This will clearly have a large social and economic impact. It is also expected that the approach undertaken by the project will be useful and applicable to other types of interdependent infrastructures.

Many different stakeholders can benefit from the CRUTIAL results:

- Electric utilities, industrial manufacturers, system integrators, etc., by designing a more resilient electric power infrastructure that benefits from dedicated information infrastructures;
- The electricity sector at large (incl. regulators), by knowing where vulnerabilities arise;
- Public authorities, by better coping with the risks associated to interdependent infrastructures;
- European citizens & industry, by continuing to enjoy the high reliability level of the electricity supply as seen in the last decades in Europe – in spite of many new evolutions in technologies and on the liberalised market.

3 DISSEMINATION ACTIONS

As underlined in the previous Section, CRUTIAL objectives are of high interest to a large sector of the population: in addition to specific stakeholders directly involved in critical utilities provisions and management, even the simple citizen would highly benefit from the project results. Therefore, the CRUTIAL activity plan includes a workpackage dedicated to disseminate project achievements and to define plans to exploit them. The partners are committed to actively promote dissemination and exploitation, at both academic and industrial level, as well as towards standardization bodies, through contacts and links they have already established and new ones to develop during the project lifetime. Moreover, the set-up of an Industrial Advisory Board constitutes a further vehicle to spread project's results to a wider community.

Dissemination implies first of all cross-fertilization among the partners, so that they can benefit from one another's technical expertise and minimize the gap of the technical approaches and schemes that are worked on at different sites. The consortium integrates leading industrial and academic researchers from three critically important, but presently only weakly connected disciplines: i) electrical power generation, transportation and distribution ii) fault-tolerant and secure real-time systems and iii) modelling and evaluation of complex systems. All three disciplines are necessary in order to pursue a separately unachievable objective, and to develop innovative solutions to the challenging problem of resilience analysis, modelling and enhancement of interdependent information and controlled power infrastructures.

The composition of the consortium has been set to ensure a well balanced and a broad coverage of all the technical areas addressed in the project. It is composed of a major research company from the electro-energetic sector and academic institutions of internationally recognised expertise and experience in all the fields of interest to CRUTIAL: design and architecture of dependability, security, fault tolerance, stochastic modelling, experimental evaluation, and deep knowledge of the target infrastructures.

Dissemination activities have been already performed and are planned for the next years in several directions. The major tools and channels used for dissemination during the project lifetime include:

- Project WWW-pages
- Workshops
- Scientific publications and conference presentations
- Publicity actions
- Promotion events by individual partners
- Liaison with other projects and programs

- Project meetings

3.1 Dissemination towards academia and the interested community at large

The project teams disseminate relevant results to the academic communities via publication and presentation of papers in the major international conferences, workshops and working groups (related to dependability, security, power system control, power system security).

Academic partners take care of the dissemination of the project results also inside the university curricula and/or in PhD courses and doctoral schools.

3.1.1 Scientific Publications

Dissemination of project's results through scientific publications (journals, magazines, conferences and workshops) in the field of dependability, security, power system control, power system security is undoubtedly an effective way to reach a wide community of both academic and industrial people interested in issues tackled by CRUTIAL. The project also disseminates the results towards the modelling and performance evaluation communities: indeed Electrical Power System Infrastructure is a rather new application field for these communities, and we expect that the interest raised by CRUTIAL papers will motivate more researchers to concentrate their efforts on the modelling of performance challenges opened up by CRUTIAL. The increasing spreading of online publications further favours the dissemination through this channel.

While journals and magazines are targeted at archival value contributions documenting research activities in specific areas, thematic conferences and workshops are particularly appealing channels for disseminating the project's results for two aspects:

- The short time between the submission of a paper and its publication in the conference/workshop proceedings. This favours quick dissemination of fresh research results
- The fruitful discussion that usually is triggered at the presentation of a paper to the conference/workshop, useful to consolidate and enhance the actual stage of the presented activities.

A list of Journals and magazines relevant for the CRUTIAL activities include:

- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Computers
- IEEE Transactions on Reliability
- IEEE Security & Privacy
- IEEE Transactions on Software Engineering
- IEEE transactions on instrumentation and measurement
- IEEE transactions on systems, man and cybernetics part C
- IEEE transactions on industrial electronics
- IEEE Internet Computing
- Computer Journal
- ACM Transactions on Information and System Security
- International Journal of Performability Engineering
- Performance Evaluation
- ACM SoSym (*Journal of Software and System Modelling*)

- International Journal of Distributed Energy Resources
- Electra, the magazine addressed to the Cigré community
- International Journal of Critical Infrastructure (IJCIS): Inderscience Publishers
- The Italian Association of Electrotechnical, Electronics, Automation, Information and Telecommunications (AEIT) Journal

A list of conferences and workshops relevant for the CRUTIAL activities include:

- International Conference on Dependable Systems and Networks (DSN)
- European Dependable Computing Conference (EDCC)
- IEEE International Symposium on Reliable Distributed Systems (SRDS)
- International Conference on Quantitative Evaluation of SysTems (QEST)
- Annual Computer Security Applications Conference (ACSAC)
- ACM/IEEE International Conference on Model Driven Engineering Languages and Systems MoDELS (was previously called "UML conference")
- IFIP WG 7.3 International Symposium on Computer Performance, Modelling, Measurements, and Evaluation (PERFORMANCE)
- ACM International Conference on Measurement and Modelling of Computer Systems – (SIGMETRICS)
- IFIP TC-11 International Information Security Conference (SEC)
- International Workshop on Critical Information Infrastructures (CRIS)
- Int. 3rd Int. Conf. on Critical Infrastructures (CRIS)
- Int. Workshop on Complex Network and Infrastructure Protection (CNIP)
- International Workshop on Research Directions for Security and networking in Critical Real-Timeand Embedded Systems (CRTES)
- IEEE Int. Conf. on Systems, Man, and Cybernetics
- Conference on Security of Information Systems - Sécurité des Systèmes d'Information (SSI)
- European Performance Engineering Workshop (EPEW)
- Modelling of Objects, Components, and Agents
- International Conference on Application of Concurrency to System Design
- The International Conference on Availability, Reliability and Security (ARES)
- International Conference on Computer Safety, Reliability and Security (SAFECOMP)
- World Computer Congress (WCC)
- IEEE Workshop on Dependable Parallel, Distributed and Network-Centric Systems (DPDNS)
- Annual Reliability and Maintainability Symposium (RAMS)
- Power Systems Computation Conference
- IEEE PES general meeting
- IEEE PES Power Systems Conference & Exposition

- IEEE Instrumentation and Measurement Technology Conference
- European Conference on Power Electronics and Applications (EPE)

So far, the CRUTIAL consortium has published a relevant number of papers; the complete lists relative to the first and second year are shown in Section 5.5 and Section 6.7, respectively.

3.1.2 Working groups related to dependability, security, power system control, power system security

IFIP WG 10.4 on Dependable Computing and Fault Tolerance http://www.dependability.org

The Working Group 10.4 of IFIP was established by the IFIP General Assembly in October 1980, and operates under IFIP Technical Committee TC-10, "Computer Systems Technology". The charter of WG 10.4 (established 1980, revised 1988) states the aim and the scope of this Working Group as follows:

Increasingly, individuals and organizations are developing or procuring sophisticated computing systems on whose services they need to place great reliance. In differing circumstances, the focus will be on differing properties of such services -- e.g., continuity, performance, real-time response, ability to avoid catastrophic failures, prevention of deliberate privacy intrusions. The notion of dependability, defined as the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers, enables these various concerns to be subsumed within a single conceptual framework. Dependability thus includes as special cases such attributes as reliability, availability, safety, security. The Working Group is aimed at identifying and integrating approaches, methods and techniques for specifying, designing, building, assessing, validating, operating and maintaining computer systems which should exhibit some or all of these attributes.

Specifically, the Working Group is concerned with progress in:

- Understanding of faults (accidental faults, be physical, design-induced, originating from human interaction; intentional faults) and their effects.
- Specification and design methods for dependability.
- Methods for error detection and processing, and for fault treatment.
- Validation (testing, verification, evaluation) and design for testability and verifiability.
- Assessing dependability through modelling and measurement.

The main goal of WG 10.4 meetings is to conduct in-depth discussions of important technical topics under the form of Workshops focusing on selected key topics. A workshop on Critical Infrastructure Protection is the main feature of the meeting to be held in January 2007.

Participants from LAAS, FCUL and ISTI-CNR are members of the IFIP WG 10.4.

A workshop on Critical Infrastructure Protection with presentations from CRUTIAL was organized jointly by Karama Kanoun, Paulo Verissimo and Rick Schlichting (AT&T Labs Research, NJ, USA) in the context of the 51st meeting of this working group held in Gosier, Guadeloupe, France, January 11-14, 2007.

IFIP Special Interest Group on Dependability Benchmarking http://www.laas.fr/~kanoun/ifip_wg_10_4_sigdeb/

Established by the IFIP WG10.4 in Summer 1999, this IFIG Special Interest Group promotes the research, practice, and adoption of benchmarks for computer-related system dependability.

In particular, the following areas are considered to be "in scope":

- Exchanging ideas about dependability benchmarking among researchers and practitioners (including participants from universities, industry, and government agencies).
- Documenting the state of the art for dependability measurement and benchmarking
- Create lists of issues that must be resolved to advance dependability benchmarking to a mature science
- Eventually, propose a mechanism and agenda for a group to propose
- As appropriate, create collaborative publications. A potential goal is to create a White Paper on dependability benchmarking as the result of this SIG's efforts.

Karama Kanoun from LAAS, a participant to CRUTIAL, is the chair of SIGDeB.

IEEE TC on Dependable Computing and Fault Tolerance http://www.dependability.org/tc/

The purpose of the Technical Committee (as exposed in its charter) is:

- Provide a forum for exchange of ideas among interested practitioners, researchers, developers, maintainers, users and students in the technical field. The goal is to promote the identification and integration of approaches, methods, and techniques for specifying, designing, building, assessing, validating, operating, and maintaining computer systems in which faults are considered as natural, anticipated events, and thus, can be tolerated. A wide variety of faults are considered, including accidental faults (physical, design-induced, or originating from human interaction) and intentional faults. Specifically, the TC is concerned with progress in:
    - the understanding of faults and their effects,
    - specification and design methods for fault-tolerant computing,
    - validation, and design for testability and verifiability, and
    - assessment, through modelling and measurement, of dependability achieved.

  In these ways, the TC hopes to play a crucial role in minimizing the risks that the increasingly sophisticated computing and communications systems might cause for society.

- Promote and facilitate the sharing of ideas, techniques, standards, and experiences between TC members for more effective use of technology.
- Conduct workshops, conferences, and other meetings to advance both the state-of-the-art and the state-of-the-practice in the technical area. This includes sponsoring the International Conference on Dependable Systems and Networks (DSN), the annual flagship activity of this TC, sponsoring annual workshops focusing on various aspects of fault-tolerant computing, and co-sponsoring relevant conferences organized by the IEEE Computer Society, the International Federation of Information Processing, and the Council of European Professional Informatics Societies.
- Publish and distribute among its members, and other IEEE-CS parties, newsletters, proceedings, standards proposals, and other appropriate material on a non-profit basis. Publish an electronic newsletter containing meeting reports, calls for papers, and news announcements.
- Provide professional development opportunities for members in the technical area and related technologies.

- Foster other activities for the advancement of the field and the interests of the TC membership within the scope of the TC's charge under the rules of the IEEE-CS, including cooperating with other groups in joint activities and projects.

Participants from LAAS, FCUL and ISTI-CNR are members of this TC.

IEEE Technical Council on Software Engineering http://www.tcse.org/.

The IEEE Technical Council on Software Engineering (TCSE) encourages the application of engineering methods and principles to the development of computer software, and works to increase professional knowledge of techniques, tools, and empirical data to improve software quality.

TCSE is involved in the myriad ways that software is designed, developed, managed, and maintained. The aim is i) to contribute to the members' professional expertise, and ii) to help advance software engineering research and practice.

The Software & Systems Engineering Standards Committee (S2ESC), one of TCSE's member committees, develops and manages IEEE software engineering standards, working under the IEEE-CS Standards Activties Board.

Other TCSE Committees (topical member groups, SIGs) bring together members worldwide to advance specialty areas within software engineering:

- Reverse Engineering and Reengineering
- Software Reliability Engineering
- Requirements Engineering
- Software Reuse
- Quantitative Methods
- Software Engineering Education
- Professional Practice

Karama Kanoun from LAAS, a participant to CRUTIAL, is a member of TCSE.

IFIP TC 11 Security and Protection in Information Systems http://www.ifip.tu-graz.ac.at/TC11/

IFIP Technical Committee on Security and Protection in Information Systems (IFIP TC11) has created in 2006 a new Working Group on Critical Infrastructure Protection (IFIP WG 11.10), chaired by Prof. Sujeet Shenoi (University of Tulsa, USA) and vice-chaired by Prof. Eric Goetz (Dartmouth College, USA). The principal aim of IFIP WG 11.10 is to weave science, technology and policy in developing and implementing sophisticated, yet practical, solutions that will help secure information, computer and network assets in the various critical infrastructure sectors. Information infrastructure protection efforts at all levels – local, regional, national and international – will be advanced by leveraging the WG 11.10 membership's strengths in sustained research and development, educational and outreach initiatives. A special session on critical information protection has been already organized by this WG in the context of the 2006 World Computer Congress (WCC-2006) during which Jean-Claude Laprie gave a presentation of preliminary models developed in the context of CRUTIAL to describe typical failures characterizing interdependent infrastructures (i.e., cascading, escalating and common-cause failures).

Yves Deswarte from LAAS is a member of the IFIP TC11 (as IEEE CS representative).). He attended the IFIP TC11 technical meeting organised at Johannesbourg, South-Africa, 14-18 May 2007.

IEEE SMC Technical Committee on Infrastructure Systems & Services (http://www.ieeesmc.org/technicalcommittess/tc_iss.html).

The mission of the TC is to contribute from a variety of disciplines, each with a different perspective on infrastructure system complexity, to an emergent theory and toolkit for the design and management of networked utility and infrastructure systems as complex socio-technical systems. In other words, the TC strives to organize a scientific stage for confronting, combining and possibly integrating the social and physical perspectives on infrastructure networks, in such a way that the insights can be made available for practitioners in the infrastructure sectors and help them to achieve better quality and reliability of infrastructure bound services.

3.2 Dissemination and Exploitation activities towards industry

The partners are committed to actively promote dissemination events towards industrial partners they have close contacts and links with, including electric power utilities, transmission system operators, power generation and distribution companies, SCADA suppliers and industry stakeholders.

A further vehicle for dissemination of CRUTIAL's results consists of the Industrial Advisory Board that the consortium has set up on the basis of active contacts, with the aim of establishing a group of advisors who will be informed about the project progress and will be invited to provide their feedbacks during the project lifetime. Actually, the IAB represents a target audience for project dissemination activities, a source of inputs about the real needs and an evaluation team of project approaches and achievements.

The plan is to have approximately one annual meeting with the IAB members, in occasion of plenary technical meetings and/or other relevant events, to promote tangible involvement and stimulate their feedbacks and advices.

The CRUTIAL consortium agrees on the importance of exploiting these channels for disseminating the CRUTIAL results.

3.3 Dissemination towards standardization bodies

Standards are a key driver in the development of engineering systems in general, and of the electric power sector in particular. As Electric Power Utilities (EPUs) have automated their operational systems, cyber-security has become a critical issue. Information & computerized instrumentation systems, used to control the electric system as well as to manage their core business and administrative tasks, face new threats and vulnerabilities along with the performance improvement provided by their growing networked interconnections and standardization. In the following, the main standard committees relevant for CRUTIAL are briefly reported.

International Electrotechnical Commission – IEC http://www.iec.ch/

IEC is an international standard organisation, which prepares and publishes international standards for all electrical, electronic and related technologies. These serve as a basis for national standardization and as references when drafting international tenders and contracts. Several IEC's Technical Committees (TCs) deal with the Critical Infrastructure issues.

The TC 65a/b/c produces standards for process control. The TC 65c is devoted to the system safety development process and its WG10 is writing a three-part international standard IEC 62443-1/2/3 on system and network security for industrial process measurement and control systems. The TC65a is working on communications in process control and started the Working Group 13 that is in charge of issuing a cybersecurity standard in Ethernet-based communications.

The TC 57 works with standards for power control systems and system components, in collaboration with other organisations making important developments with respect to SCADA security, such as the American Gas Association (AGA), the Instrumentation, Systems and Automation Society (ISA) and NIST (the USA's National Institute of Standards and Technology). It is composed of a relevant set of working groups, among them: telecontrol protocols, distribution automation, substation communication, application program interface for Energy Management Systems, communication for deregulated energy markets, interfaces for distribution management systems, interoperability, data and communication security. The WG 15 is specifically related to Data and Communication security and has published a white paper “IEC TC57 Security Standards for the Power System’s Information Infrastructure – Beyond Simple Encryption”.

International Council on Large Electric Systems – CIGRÉ http://www.cigre.org/

CIGRÉ includes several study committees (SCs), facilitating international exchange on knowledge in the electricity industry. At least three of these committee deal with issues, which are related to Critical Infrastructure:

- SC B3 – Substations: includes adoption of technological advances in equipments and systems in order to improve reliability and availability.
- SC C2 – System Operation and Control: considers functionalities and assesses security in operation of Control systems.
- SC D2 – Information Systems and Telecommunication: monitors emerging technologies and focuses on security requirements in the ICT-related systems.

The aforementioned SCs convened in 2003 the Joint Working Group titled “Security for Information Systems and Intranets in Electric Power Systems” that produced a series of papers in the journal Electra for raising awareness in the sector. In summer 2006, the JWG D2/B3/C2-01 ended its activities and the new Working Group 22 within the SC D2” has been set up at the meeting held in Paris in August 2006. The new WG titles “Treatment of Information Security for Electric Power Utilities (EPUs)” and will continue the work started by the previous JWG following three main discussion tracks:

- Security Management Frameworks
- Risk Assessment
- Security Technologies.

Giovanna Dondossola is a member of D2.22, chairing the discussion on the Risk Assessment track.

Process Control System Forum - PCSF www.pcsforum.org

The PCSF is an open, collaborative, voluntary forum of international stakeholders from government; academia; industry users, owner/operators, and systems integrators; and the vendor community. Its main objective is to establish a Forum for the control systems community that is uniquely positioned to:

- Aggregate information about current organizations, their efforts, directions, and work product from across multiple sectors to increase visibility and reduce redundancy.
- Identify consensus cross-industry and cross-functional issues that require resolution, and determine a path and effort that is owned, traceable, and produces generally acceptable solutions.
- Cross-connect decision-makers from industry, government, vendors, and academia, in ways that promote increased understanding of requirements and opportunities for collaboration.
- Impact a broad portion of the control system community through procedures, methods, guidelines, best practices, and other resources, issued through organizations that participate in the PCSF.

The currently active PCSF WGs are the following:

Standards	Standards committee chairs coordinate to avoid duplicative or

Awareness	conflicting standards.
Control System Security Event Monitoring	Detecting cyber attacks on DCS and SCADA systems that run the critical infrastructure.
SCADA Cyber Self-Assessment	The goal of SCySAG is to enable the development and use of the best possible next generation of self administered tools and methodologies for the assessment of the cyber security readiness of the process control systems. These systems are used in manufacturing, industrial, energy, and utilities. Specifically, SCySAG will publish and publicize methodology and tool requirements information, as well as objective data about available tools and methodologies.

Many electric power utilities are aware of this evolution and are structuring their approaches accordingly. Common cybersecurity frameworks, that is to say, comprehensive approaches to manage risks adequately and create a common ground to build adapted defences and security processes, are necessary to adopt an efficient and coherent enterprise-wide response. The establishment of such frameworks can be done based on several existing standards, which differ in their nature (e.g. informational, regulatory, compliance-oriented, etc.), in their form (guidelines, reports…), and also in their scope. The different contributons may be grouped under the following categories:

- general IT, such as the ISO/IEC 2700x series, including **ISO 27002** (formerly ISO 17779); the **NIST** Risk Management Framework (NIST SP 800-60 ; **SP 800-53** ; SP 800-30 ; SP 800-18 ; SP 800-70 ; SP 800-53A ; SP 800-37) and its associated security standards and guidance (**NIST SP800-82**); **ISO/IEC 15448** (Common Criteria);
- process control-oriented, such as **ISA SP99** (Manufacturing and Control Systems Security Standards); **IEC 62443** (Security for Industrial Process Measurement and Control – Network and System Security standard ; by IEC TC65C WG10); the British **CPNI**- Good Practice Guide - Process Control and SCADA Security Guides; Future Adaptation of the NIST SP 800-53 for ICS; NIST ICC-SPP / PCSRF; API (American Petroleum Institute) 1164;
- electrical generation, transmission and distribution-oriented, such as **IEC 62351** (Power systems management and associated information exchange - Data and communication security ; by IEC TC57WG15); the **NERC (**North America Electric Reliability Council) **CIP** standards; IEEE P1689; IEEE P1711; IEEE 1402; Secure DNP3 / DNP User Group.

A comparison of existing cybersecurity standards for Electric Power Utilities is being prepared by the Cigré D2.22 working group and will be published at the next Cigrè Session 2008. This paper will provide an overview and analysis of existing work which an electric power utility can consider in order to define appropriate security approaches for its specific needs.

The standardisation bodies, related to power control systems, presented above are one type of industrial community targeted by our dissemination actions. Partners already involved in working groups on standardization will take the opportunity of WG meetings for disseminating project results, and to understand the trends inside the community as useful feedback for the project.

Standardization bodies in the field of cyber security of power control systems will take advantage of CRUTIAL results. CESI-R commits to interact and disseminate CRUTIAL's results to the benefit of those standardization bodies through its direct participation to the already mentioned Cigré WG D2.22.

3.4 Project's technical meetings

Project meetings are the main events for internal dissemination within the project. In addition, they also serve as a tool for disseminating information within the partner organisations.

It has been agreed that partners in turn will host the project meetings.

3.5 Thematic workshop

The project participants will support the organisation of a thematic workshop, to showcase the research and technology solutions pioneered by the project. The involvement will be mainly in producing and presenting papers describing the CRUTIAL activities and results, by participating in the technical programme committee, chairing sessions, etc. To raise the attendance and thus increase the dissemination level of project results, such event, to be held during the second half of the project lifetime, is planned in conjunction with a relevant related conference and/or similar workshops run by related projects. Contributions will be solicited also from the community outside the project participants, especially from the involved members of the IAB, to promote fruitful cross fertilization. This event is going to be finalised soon. A possibility under discussion inside the consortium is to organise this event in conjunction with the 4th International Conference on Critical Infrastructures to be held in 2008.

4 LIAISON WITH OTHER PROJECTS AND PROGRAMS

The project partners have also agreed to establish strong and fruitful links with other related international projects. In fact, vulnerability of critical infrastructure appears to be growing due to a number of factors, including growing demand, hectic transactions, growing number of stakeholders, high interconnection and interdependencies, complexity of control. Therefore, development of integrated interdisciplinary frameworks and related technologies for the provision of resilience, dependability and security in complex interconnected and heterogeneous communication networks and information infrastructures that underpin our economy and society is being prioritised by research workprogramme, both at European and American levels.

The CRUTIAL consortium is aware of a number of related programmes/projects/initiatives, briefly presented in the following, and has established contacts with some of them, especially other European projects, to benefit of reciprocal research advances in the targeted field of electrical power utilities and, more in general, in the field of resilient and secure infrastructure systems. Cooperation is mainly realized in terms of exchange of activity documents and participation to relevant events (such as thematic workshops organized by such projects).

4.1 Related European Projects

Among the most relevant R&D projects related with CRUTIAL there are those supported by the EU under the FP6-IST Programme Projects in the Strategic Objective *"Towards a global dependability and security framework"* (http://cordis.europa.eu/ist/trust-security/projects.htm) and listed in Table 1. They belong to the categories of Integrated Projects, Network of Excellence, Specific Targeted Research Projects and Coordination Actions.

IRRIIS, GRID and CI2RCO are EU projects focusing on Critical Infrastructure Protection and therefore highly related to CRUTIAL.

The IRRIIS project aims at increasing the dependability and resilience of Large Complex Critical Infrastructures by introducing appropriate Middleware Improved Technology (MIT) based on Information and Communication Technology (ICT). The focus of the project is highly related to that of CRUTIAL, being on electricity and telecommunications and especially on the interdependencies between these infrastructures, analyzed through the development of a synthetic simulation environment (SYNTEX).

The objective of GRID is to achieve consensus at the European level on the key issues involved by power systems vulnerabilities and the relevant defence methodologies, in view of the challenges driven by the transformation of the European power infrastructure. GRID wants to assess the needs of the EU power sector on these issues and achieve consensus among stakeholders and R&D institutions, so as to establish a roadmap for collaborative research in view of the forthcoming 7th framework programme. The focus is especially directed to: i) methods to assess reliability, security and risks affecting the power grid, and ii) management, control and protection schemes and the relevant architectures and devices.

Title	Type	Start date-End date	Website
IRRIIS – Integrated Risk Reduction of Information-based Infrastructure Systems	EU IP Project – Funded under FP 6	01/02/2006 31/01/2009	http://www.irriis.org/
GRID: a coordination action on ICT vulnerabilities of power systems and the relevant defence methodologies	EU CA Project – Funded under FP 6	01/01/2006 31/12/2007	http://grid.jrc.it/
CI2RCO - Critical information infrastructure research coordination	EU CA Project – Funded under FP 6	01/03/2005 28/02/2007	http://www.ci2rco.org
ReSIST - Resilience for survivability in IST	EU NoE Project – Funded under FP 6	01/01/2006 31/12/2009	http://www.laas.fr/RESIST
SERENITY: System Engineering for Security and Dependability	EU IP Project – Funded under FP 6	01/01/2006 31/12/2008	www.serenity-project.org
DESEREC: Dependability and Security by Enhanced Reconfigurability	EU IP Project – Funded under FP 6	01/01/2006 31/12/2008	www.serenity-project.org
HIDENETS - HIghly DEpendable ip-based NETworks and Services	EU STREP Project – Funded under FP 6	01/01/2006 31/12/2008	www.hidenets.aau.dk
ESFOR -: European Security Forum for web services, software, and systems	EU CA Project – Funded under FP 6	01/11/2005 31/10/2007	www.esfors.org
SECURIST - Security IST Projects Cluster Support	EU CA Project – Funded under FP 6	01/11/2004 31/10/2006	www.ist-securist.org

Table 1: EU projects related to CRUTIAL

The main objective of the CI2RCO project was to create and coordinate a European Taskforce to i) encourage a co-ordinated Europe-wide approach for research and development on Critical Information Infrastructure Protection (CIIP), and ii) to establish a European Research Area (ERA) on CIIP as part of the larger IST Strategic Objective to integrate and strengthen the ERA on Dependability and Security. CI2RCO focussed on activities across the EU-25 and ACC[1] that are essential to be carried out at European level and that require collaborative efforts involving the relevant players of research, research funding actors, policy-makers and CI-stakeholders. This has been accomplished by a set of coordination activities supporting the improvement of networking and coordination of national and European research policies, programmes and funding schemes.

The CRUTIAL consortium has already promoted cooperation with these projects, mainly in terms of exchange of activity documents and participation to relevant events (such as thematic workshops organized by these projects). There are already strong links by some

[1] ACC means: Acceding and Candidate Countries

CRUTIAL partners: KUL is a partner in the GRID project, and belongs to the advisory board of the CI2RCO project; CESI-R is a partner in the GRID project. Of course, they will act as a highly effective vehicle for cross-fertilization among related activities. Moreover, the CRUTIAL consortium is part of the “IRRIIS Interest Group”.

The other EU projects listed in Table 1 do not focus on Critical Infrastructures Protection, but include it in a wider perspective embracing resiliency and securtity in ICT systems. There are already established links with some of these projects, mainly through the direct participations of CRUTIAL. In fact:

- FCUL is a partner in the ReSIST, HIDENETS, ESFORS and SECURIST projects;
- LAAS is a partner in the ReSIST and HIDENETS projects;
- Some members of the ISTI-CNR team are involved in the ReSIST and HIDENETS projects.

4.2 Other initiatives

In Table 2, some other initiatives related to CRUTIAL are listed.

Title	Type	Start date-End date	Website
PolSec - Politiques de sécurité et contrôle d’accès pour les grandes infrastructures critiques	Collaborative research project between LAAS-CNRS and LIFO «Laboratoire d'Informatique Fondamentale d'Orléans», France	Jan 2006 Dec 2008	http://www2.laas.fr/PolSec/
RDS - Ricerca di Sistema	Italian Research Programme - Funded by the Italian Ministry of Industry, Trade and Crafts	Active since 2000	http://www.ricercadisistema.it/
TCIP: Trustworthy Cyber Infrastructure for the Power Grid	US project – Funded by NSF, Dep. of Energy and Dep. of Homeland Security	August 2005 August 2010	http://www.iti.uiuc.edu/tcip/

Table 2: Other initiatives related to CRUTIAL

The Italian Research Programme RdS has been set-up within the frame of the Public Interest Energy and performs research and development activities aimed at improving the economics, security and quality of the Italian electric system. The objective is to devise solutions to practical problems, taking into account dynamic evolutions and sustaining the changes dictated by international agreements (Kyoto), and evaluating the scientific-technological progresses. From 2000 to 2005 CESI (Centro Elettrotecnico Sperimentale Italiano) had been appointed to manage the funds assigned to the projects and its personnel (now moved in CESI RICERCA) were deeply involved in the development of the research activities. This Research Programme is structured into projects co-participated by the major research operators in the electrical field and academics, whose results are made public in form of reports (in Italian) or published papers (in Italian and English). The Programme covers a wide-scope area of research in power generation, transmission and distribution grids, renewable and dispersed energy sources, also considering the physical hazards and environmental impact of these installations. Of specific interest for CRUTIAL are the activities in the area of power system regulation, control and automation including new control criteria for the power grids, probabilistic approaches to static and dynamic security assessment in the preventive control, ICT security analysis methodologies and robust ICT architectures that support the design and operation of networked automation applications, menaced by both accidental and malicious ICT faults. Through the direct involvement of CESI RICERCA, the CRUTIAL consortium is strongly connected with related RdS activities.

The TCIP NSF Cyber Trust Center is a US initiative created in August 2005 to address the challenge of how to protect the US power grid. TCIP is working to provide the fundamental science and technology needed to create an intelligent, adaptive power grid that can survive malicious adversaries, provide continuous delivery of power, and support dynamically varying trust requirements. The objective is to develop the necessary cyber building blocks and architecture, and the validation technology to quantify the amount of trust provided by the proposed approach. TCIP Focus Areas include: i) Reliable and Secure Computing Base; ii) Trustworthy Data Communications and Control; iii) Wide-area Trustworthy Information Exchange, and iv) Quantitative validation. Given the highly related objectives of the two projects, CRUTIAL will promote liaison with TCIP. The workshop on Critical Infrastructure Protection organized by the IFIP WG 10.4 on January 2007 in Guadeloupe, France, with presentations from members of both CRUTIAL and TCIP, was a valuable opportunity for exchanging on the ongoing activities and crossfertilization.

The aim of PolSecis is to develop access control policies and models as well as protection mechanisms, including for authentication and authorization, that are well suited to address the challenges raised by large, open, heterogeneous and interdependent critical information infrastructures. In particular, these models and mechanisms should take into account the various organizations involved in the infrastructure and the various roles of the users belonging to these organizations. These mechanisms should be able to enforce a global security policy, defined from the security policies of the various organisations. Through the direct participation of LAAS, the electric power infrastructures and the associated information and control infrastructures, such as those investigated in CRUTIAL, are used as an example in this project. Nevertheless, the objective is to develop security models and protection mechanisms that are also suitable to other application domains.

5 DISSEMINATIONS ACTIONS UNDERTAKEN DURING THE FIRST YEAR

The dissemination actions undertaken during the first year have addressed several dissemination channels among those identified in the previous sections.

5.1 Project Web site

The project has established a web site http://crutial.cesiricerca.it/ supported by the project partners and maintained by the coordinator, to provide a unified view of the project and to present CRUTIAL to the international community. The project WWW-pages serve as a means for continuous dissemination of information about the project for the public awareness as well as internally for the project participants. It is structured in two major areas: a public section and a private section. The public section offers general information on the project, including all public deliverables and other public documents produced in the framework of the project. Special attention is intended to be given to the quality of the WWW-pages and their frequent updating. The reserved area contains material accessible by project partners only, mainly working documents and any other material considered useful to the project partners. Two additional private web areas have been also set up: one reserved to the Industrial Advisory Board (IAB) members and the other for the European Commission. The IAB area allows to access some project presentations and documents (e.g., the material from the joint CRUTIAL & Cigré Session that was held in conjunction with the 2nd Technical Meeting in Leuven in May 2006). The EU area makes visible the material requested by the Commission, such as public and restricted project deliverables.

5.2 Dissemination and Exploitation activities towards industry

The planned Industrial Advisory Board has been set up; the current members are:

- SIEMENS
    - Claus Kern Claus.Kern@siemens.com

  - Michael Munzert michael.munzert@siemens.com
- ScottishPower
  - Bill Fulton Bill.Fulton@sppowersystems.com
- EFACEC
  - Antonio Manuel Carrapatoso amc@se.efacec.pt
- Statnett
  - Tor Aalborg tor.aalborg@statnett.no
- ENEL Distribuzione
  - Fiorenza Gennaro gennaro.fiorenza@enel.it
- Svenska Kraftnat
  - Goran N. Ericsson goran.n.ericsson@svk.se
- Salten Kraftsamband
  - Age Torkilseng age.torkilseng@sks.no

During this first year of the project, there has been the opportunity to co-locate the second plenary technical meeting of CRUTIAL with a meeting of the CIGRE' WG D2/B3/C3-01. It was in May 2006, in Leuven, Belgium. A special session was therefore planned in the agenda of the CRUTIAL technical meeting to this purpose. For the industrial side, 4 Cigré members (including the CRUTIAL coordinator, Dr. Dondossola) and 1 member of the Industrial Advisory Board attended the meeting. The Session was organised into an overview of the CRUTIAL project, followed by one presentation per each WP and by a final presentation by the Cigré Convenor. After the presentations there was a discussion about the opportunity of collaborating with JWG in the identification of further works to be suggested by the JWG Technical Brochure, currently under preparation.

Following the CRUTIAL/Cigré Session two Cigré members accepted to join the CRUTIAL IAB team.

5.3 Presentations related to CRUTIAL and further dissemination actions

Presentations have been made by project members at the following events:

- G. Deconinck,“Opportunities for intelligent communication networks in distributed electricity generation”, CRIS technical meeting (Critical Infrastructure Institute), CPRI (Central Power Research Institute), Bangalore, India, Feb. 14, 2006.
- G. Deconinck, “Bedreigingen voor security in de process industrie – conceptueel kader en trends,” Agoria/TI-BIRA seminar on Security in de procesindustrie – meer dan hackers buitenhouden, Ter Elst, Edegem, 21 Feb. 2006 (in Dutch).
- Paulo Verissimo, NSF-US workshop on “Beyond SCADA: Networked Embedded Control Systems Planning Meeting”, which took place in Washington DC on 14-15 March, 2006.
- Paulo Verissimo, “On resilience of modern critical infrastructures”, Joint EU-US workshop on “Large ICT-based Infrastructures and Interdependencies: Control, Safety, Security and Dependability”, which took place in Washington DC on 16-17 March, 2006.
- Giovanna Dondossola, SecurIST workshop - Integration of 'New' D4 Projects with SecurIST, held in Brussels on 22 March, 2006.
- Yves Deswarte,"Les systèmes de commande face à la malveillance: quelles solutions pour quelles menaces?", Seminar "La cyber-sécurité des systèmes de contrôle", Working Group SP99, ISA-France, Nice , 10-11 May, 2006 (in French).
- G. Deconinck, “Netwerkkoppelingen – niets dan voordelen !?,” Profibusdag 2006, Keynote lecture, Ter Elst, Edegem, 1 Jun. 2006 (in Dutch).

- Paulo Verissimo, “Security challenges in systems-of-embedded-systems”, at the Joint US-EU-TEKES workshop: Long Term Challenges in High Confidence Composable Embedded Systems, Helsinki, Finland, June 2006.
- Jean-Claude Laprie, "Modelling Outages in Independent Critical Infrastructure", IFIP WG 10.4 50th meeting, Annapolis, Maryland, USA, 28 June, 2 July, 2006.
- Felicita Di Giandomenico, "Overview of the CRUTIAL challenges and objectives", IFIP WG 10.4 50th meeting, Annapolis, Maryland, USA, 28 June, 2 July, 2006.
- Jean-Claude Laprie, "Opening of the electricity market: an exacerbation of the interdependencies between the electricity and information infrastructures, 19th IFIP World Computer Congress (WCC-2006), Special Session on Critical Infrastructure Protection, Santiago, Chile, August 20-25, 2006.
- Giovanna Dondossola, “Presentation of CRUTIAL” CRIS (Critical Infrastructure Institute) Third International Conference on Critical Infrastructures, Panel Session on Critical Infrastructure Protection, which took place in Old Town Alexandria (Virginia, USA) on 24-27 September, 2006.
- Jean-Claude Laprie, "Dependability of Critical Infrastructures- Modelling interdependencies between the Electricity and Information Infrastructures", joint meeting between LAAS and JST-CRDS (JAPAN), LAAS-CNRS, October 23, 2006.
- Mohamed Kaaniche, "Presentation of CRUTIAL", joint meeting between LAAS and JST-CRDS (JAPAN), LAAS-CNRS, October 23, 2006.
- Anas Abou El Kalam, Yves Deswarte (invited speakers), "Access Control for Critical Infractructures", VI International Congress on Secure telematic applications in national and international projects, november 22-24, 2006, Minsk.
- Jean-Claude Laprie, "Presentation of CRUTIAL", Networking Session on Resilient Infrastructures and Information Fusion for Security: Current approaches, challenges and future directions, IST Event 2006, 21-23 November 2006, Helsinki, Finland.

Also, it is worth mentioning the initiative undertaken by the Electricity Group of the "Energy production and distribution systems" Unit from DG Research, which reviewed the **European projects in the Electricity field**, by preparing a brochure presenting the **synopses of relevant projects in this area**, in view of the upcoming **7th Framework Programme**. CESI RICERCA contributed to this initiative by preparing the CRUTIAL synopsys to be included in this brochure.

5.4 Project’s technical meetings

During the first year, 3 plenary meetings have been held:

1st Technical Meeting, February 22-23, Milan, hosted by CESI-R (it acted also as kick-off meeting)

2nd Technical Meeting, May 16-17, Leuven, hosted by KUL;

3rd Technical Meeting, October 16-17, Lisboa, hosted by FCUL.

All the three meetings have been well attended by all the partners, and have been very useful forums for creating a common project knowledge and view on the basis of the individual expertise of the participants, for discussing research directions in a coordinated and cooperative manner, for showing and discussing the advancements from the previous meeting and getting feedbacks for improvements/extensions. The agenda for the1st and 3rd events have also included an Executive Board Meeting session, for discussing the major issues related with the implementation of the workplan.

5.5 Collection of Publications relative to the first year

5.5.1 Publications explicitly acknowledging the support of the CRUTIAL project.

Journals:

[1] Miguel Correia, Nuno Ferreira Neves, Paulo Veríssimo, "From Consensus to Atomic Broadcast: Time-Free Byzantine-Resistant Protocols without Signatures", The Computer Journal, Vol. 49, No. 1, pages 82-96, Oxford University Press, January 2006.

[2] J. Sproston and S. Donatelli, "Backward Bisimulation in Markov Chain Model Checking", IEEE Transactions on Software Engineering, August 2006, vol.32, n. 8, pp.531-546.

Conference Proceedings:

[3] G. Dondossola, G. Deconinck, F. Di Giandomenico, S. Donatelli, M. Kaâniche, P. Verissimo, "Critical Utiliy Infrastructural Resilience", International Workshop on Research Directions for Security and Networking in Critical Real-Time and Embedded Systems (CRTES 06), San Jose (USA), 4 April 2006, 4 pages.

[4] G. Dondossola, G. Deconinck, F. Di Giandomenico, S. Donatelli, M. Kaâniche, P. Verissimo, "Critical Utiliy Infrastructural Resilience", Proc. Int. Workshop on Complex Network and Infrastructure Protection (CNIP-2006), Rome, Italy, 28-29 Mar. 2006, pp. 183-195. Also in PCSF Reference Library (<https://www.pcsforum.org/library>).

[5] T. Rigole, K. Vanthournout, G. Deconinck, "Interdependencies between an Electric Power Infrastructure with Distributed Control, and the Underlying ICT Infrastructure", Proc. Int. Workshop on Complex Network and Infrastructure Protection (CNIP-2006), Rome, Italy, 28-29 Mar. 2006, pp. 428-440.

[6] T. Rigole, G. Deconinck, "A survey on modelling and simulation of interdependent critical infrastructures," *Proc. 3rd IEEE Benelux Young Researchers Symposium in Electrical Power Engineering*, Gent, Belgium, April 27-28, 2006; 9 pages

[7] J.C. Laprie, K. Kanoun, M. Kaaniche, "Modelling cascading and escalading outages in Interdependent Critical Infrastructures", Fast Abstract in Supplement of the International Conference on Dependable Systems and Networks (DSN), Philadelphia, USA, June 2006.

[8] N. Ferreira Neves, "Locating File Processing Vulnerabilities", Fast Abstract in Supplement of the International Conference on Dependable Systems and Networks (DSN), Philadelphia, USA, June 2006.

[9] Nuno Ferreira Neves, João Antunes, Miguel Correia, Paulo Veríssimo, Rui Neves, "Using Attack Injection to Discover New Vulnerabilities", in Proceedings of the International Conference on Dependable Systems and Networks (DSN), Philadelphia, USA, June 2006.

[10] Henrique Moniz, Nuno Ferreira Neves, Miguel Correia, Paulo Veríssimo, "Randomized Intrusion-Tolerant Asynchronous Services", in Proceedings of the International Conference on Dependable Systems and Networks (DSN), Philadelphia, USA, June 2006.

[11] A.N.Bessani and M.Correia and J.S.Fraga and L.C.Lung. Sharing Memory between Byzantine Processes using Policy-Enforced Tuple Spaces. In Proceedings of the 26th International Conference on Distributed Computing Systems (ICDCS), July 2006.

[12] Paulo Veríssimo, Nuno Ferreira Neves, Miguel Correia, CRUTIAL: The Blueprint of a Reference Critical Infrastructure Architecture, Proceedings of the 1st International Workshop on Critical Information Infrastructures Security (CRITIS), Samos Island, Greece, August 2006.

[13] Bondavalli, S. Chiaradonna, P. Lollini, and F. Squittieri, “Integration of an MPS modelling approach into Möbius”, 3rd International Conference on Quantitative Evaluation of SysTems (QEST 2006) - Tool Session, University of California, Riverside, CA, USA, September 2006.

[14] M. Garetto, M. Gribaudo, “Performance analysis of delay tolerant networks with model checking techniques”, 3rd International Conference on Quantitative Evaluation of SysTems (QEST 2006) - University of California, Riverside, CA, USA, September 11-14, 2006.

[15] D. Cerotti, S. Donatelli, A. Horváth, J. Sproston, “CSL model checking for generalized stochastic Petri nets”, 3rd International Conference on Quantitative Evaluation of SysTems (QEST 2006) - University of California, Riverside, CA, USA, September 11-14, 2006.

[16] M. Beccuti, G. Franceschinis, S. Baarir, J.-M. Ilié “Efficient lumpability check in partially symmetric systems” 3rd International Conference on Quantitative Evaluation of SysTems (QEST 2006) - University of California, Riverside, CA, USA, September 11-14, 2006.

[17] G. Dondossola, G. Deconinck, F. Di Giandomenico, S. Donatelli, M. Kaâniche, P. Verissimo, “An Approach to Modelling and Mitigating Infrastructure Interdependencies”, Proc. 3rd Int. Conf. on Critical Infrastructures (CRIS-2006), Old Town Alexandria (VA), USA, September 25-27, 2006, 4 pages.

[18] Alessandro Daidone, Felicita Di Giandomenico, Andrea Bondavalli, Silvano Chiaradonna, “Hidden Markov Models as a support for diagnosis: formalization of the problem and synthesis of the solution”, in Proceedings 25th IEEE SRDS Conference, Leeds, UK, October 2006.

[19] Henrique Moniz, Nuno Ferreira Neves, Miguel Correia, Paulo Veríssimo, Experimental Comparison of Local and Shared Coin Randomized Consensus Protocols, Proceedings of the 25th IEEE Symposium on Reliable Distributed Systems (SRDS), Leeds, UK, October 2006.

[20] Paulo Sousa, Nuno Ferreira Neves, Paulo Veríssimo, William Sanders, Proactive Resilience Revisited: The Delicate Balance Between Resisting Intrusions and Remaining Available, Proceedings of the 25th IEEE Symposium on Reliable Distributed Systems (SRDS), Leeds, UK, October 2006

[21] G. Deconinck, T. Rigole, K. Vanthournout, R. Tirtea, A. Dusa, J. Driesen, “Embedded automation for energy applications and its interdependence with the info'structure”, Proc. 2006 IEEE Int. Conf. on Systems, Man, and Cybernetics, (special session: The security challenge of public information networks in operation of industrial systems and critical infrastructures), Taipei, Taiwan, 8-11 October 2006, pp. 575-579.

[22] Eric Alata, V. Nicomette, M. Kaaniche and M. Dacier, "Lessons learned from the deployment of a high-interaction honeypot", Proc. Sixth European Dependable Computing Conference (EDCC-6), Coimbra, Portugal, October 18-20, 2006, IEEE Computer Society, pp. 39-44

[23] Anas Abou El Kalam, Yves Deswarte, "Multi-OrBAC: a new access control model for distributed, heterogeneous and collaborative systems", 8th International Symposium On Systems And Information Security (SSI’2006), 08-10 November 2006, Sao Jose Dos Campos, Sao Paulo, Brazil.

[24] T. Rigole, K. Vanthournout, G. Deconinck, “Distributed control systems for electric power applications” *Proc. 2nd Int. Workshop on Networked Control Systems: Tolerant to Faults,* Rende (CS), Italy, 23-24 Nov. 2006, 7 pages.

[25] T. Rigole, G. Deconinck, G. Dondossola, F. Garrone, C. Brasca, “Impact of ICT failures on distributed generation applications,” *Proc. DIGESEC - CRIS workshop 2006 Influence*

of distributed generation and renewable generation on power system security, Magdeburg, Germany, 6-8 Dec. 2006.

[26] D. D'Aprile, S. Donatelli, A. Sangnier, J. Sproston. "From Time Petri Nets to Timed Automata: an Untimed Approach", accepted for publication at TACAS 2007 (13th. International Conference on tools and Algorithms for the Construction and Analysis of Systems).

5.5.2 Publications related to CRUTIAL activities but without explicit acknowledgement to CRUTIAL

[1] G. Dondossola, O.Lamquet, J. Szanto, "Sicurezza delle comunicazioni nei sistemi d controllo del sistema elettrico", The Italian Association of Electrotechnical, Electronics, Automation, Information and Telecommunications (AEIT) Journal, No. 1, pages 16-27, January/February 2006 (in Italian).

[2] G. Dondossola, J. Szanto, M. Masera, I.N. Fovino, "Evaluation of the effects of intentional threats to power substation control systems", Proc. Int. Workshop on Complex Network and Infrastructure Protection (CNIP-2006), Rome, Italy, 28-29 Mar. 2006, pp. 309-320. Also selected for publication on the Special Issue of the International Journal of Critical Infrastructures (IJCI).

[3] M.Martinello, M. Kaaniche, K. Kanoun, Aguilar-Melchor, "Modelling user perceived unavailability due to long response times", 11th IEEE Workshop on Dependable Parallel, Distributed and Network-Centric Systems (DPDNS'06), Rhodes (Greece), 25-29 April 2006, pp. 163-183 □

[4] S. Bernardi, J. Merseguer, "QoS assessment via Stochastic Analysis", IEEE Internet Computing, vol. 10(3), May 2006, pp. 32-42.

[5] M. Martinello, M. Kaaniche, K. Kanoun, Modelling service availability in web clusters architectures, Workshop on Fault Tolerant Computing (WTF'2006), Curitiba (Brésil), 29 May - 2 June, 2006, pp. 93-106.

[6] A. Abou El Kalam, Y. Deswarte, "Multi-OrBAC: un modèle de contrôle d'accès pour les systèmes multi-organisationnels", Third Conference on Security of Information Systems - Sécurité des Systèmes d'Information (SSI 2006), Seignosse (France), 6-9 June 2006 (in French).

[7] A. Horváth, M. Telek Editors, "Formal Methods and Stochastic Models for Performance Evaluation", Third European Performance Engineering Workshop, EPEW 2006, Budapest, Hungary, June 21-22, 2006, Proceedings LNCS 4054, Springer.

[8] D. Codetta-Raiteri, G. Franceschinis, M. Gribaudo, "Defining formalisms and models in the DrawNet modelling system", Workshop on Modelling of Objects, Components, and Agents, (MOCA2006), Turku, Finland, June 2006.

[9] S. Donatelli and P.S. Thiagarajan Editors, "Proceedings of the 27th International Conference on Application and Theory of Petri Nets and Other Models of Concurrency", Turky, Finland, June 26-30 2006, LNCS 4024, Springer.

[10] L.C.Lung and F.Favarim and G.T.Santos and M.Correia. An Infrastructure for Adaptive Fault Tolerance on FT-CORBA. In 9th IEEE Proceedings of the International Symposium on Object and component-oriented Real-time distributed Computing (ISORC). June 2006.

[11] L. Gonczy, S. Chiaradonna, F. Di Giandomenico, A. Pataricza, A. Bondavalli, T. Bartha, "Dependability Evaluation of Web Service-Based Processes", in Formal Methods and Stochastic Models for Performance Evaluation: Third European Performance Engineering Workshop, EPEW 2006, Budapest, Hungary, June 21-22, 2006. Proceedings, Lecture Notes in Computer Science, Vol. 4054/2006, pp. 166-180.

[12] M. Martinello, M. Kaaniche, K. Kanoun, C.Aguilar-Melchor, Modelling service unavailability due to long response time for single and multi server queueing systems, XXVI Congresso da Sociedade Brasileira de Computaçao Tecnologia da Informaçao e Desenvolvimento Regional, Campo Grande (Brésil), 14-20 July, 2006.

[13] D. Cerotti, D. D'Aprile, S. Donatelli and J. Sproston, "Verifying Stochastic well-formed nets with CSL Model-Checking Tools", in K. Goossens and L. Petrucci (editors), *Proceedings of the 6th International Conference on Application of Concurrency to System Design (ACSD'06)*. © IEEE Computer Society press 2006.

[14] S. Montani, L. Portinale, A. Bobbio, D. Codetta Raiteri, "Automatically Translating Dynamic Fault Trees into Dynamic Bayesian Networks by Means of a Software Tool" ARES 2006, pp. 804-809.

[15] G. Dondossola, O.Lamquet, A. Torkilseng, " Key issues and related methodologies in the security risk analysis and evaluation of electric power control systems", in 2006 Cigré Session, Study Committee D2 "Information, Telecommunication and Telecontrol systems in the Electric Power Industry", Paris, FR, September 2006.

[16] Ana-Elena Rugina, Karama Kanoun, Mohamed Kaaniche, "Modélisation de la sûreté de fonctionnement de systèmes à partir du langage AADL", 15eme Congrès International Maîtrise des Risques et Sûreté de fonctionnement (Lambda-mu 15), Lille, France, 10-12 Oct. 2006.

[17] Ana-Elena Rugina, Karama Kanoun, Mohamed Kaaniche, "An Architecture-based Dependability Modelling Framework using AADL", 10th IASTED International Conference on Software Engineering and Applications, (SEA 2006), Dallas, TX, USA, 13-15 Nov 2006.

[18] G. Deconinck, R. Belmans, J. Driesen, B. Nauwelaers, E. Van Lil, "Reaching for 100% reliable electricity services: multi-system interactions and fundamental solutions," *Proc. DIGESEC - CRIS workshop 2006 Influence of distributed generation and renewable generation on power system security,* Magdeburg, Germany, 6-8 Dec. 2006.

[19] D. Codetta-Raiteri. "BDD based analysis of Parametric Fault Trees". In Proceedings of the Annual Reliablity and Maintainability Symposium, Newport Beach (CA USA), pp. 442-449, 2006.

[20] Miguel Correia, Nuno Ferreira Neves, Lau Cheuk Lung, Paulo Veríssimo. Worm-IT - A Wormhole-based Intrusion-Tolerant Group Communication System. Journal of Systems & Software, Elsevier, accepted for publication.

6 DISSEMINATIONS ACTIONS UNDERTAKEN DURING THE SECOND YEAR

6.1 Project Web site

The project web site, already set up during the first months after the starting of the project, has been maintained by CESI-R. The project WWW-pages constitute an important means for continuous dissemination of information about the project for the public awareness as well as internally for the project participants. It has been regularly updated by the partners with information useful to fulfil the objective of both intra consortium dissemination as well as external dissemination.

6.2 Presentations related to CRUTIAL and further dissemination actions

Presentations have been made by project members at the following events:

1. Giovanna Dondossola, "Risk Assessment in the Electric Power Industry" Cigré meeting - WG D2.22 "Treatment of Information Security in the Electric Power Utilities (EPUs)", Swiss Grid, Zurich 20 February 2007.

2. Giovanna Dondossola, “CRUTIAL-CRitical UTility InfrastructurAL resilience”, Governo e Sicurezza delle Grandi Reti Tecnologiche ed Energetiche – presentazione di alcuni risultati delle attività di ricerca in Italia Workshop ENEA, Rome 22 June 2007.
3. Giovanna Dondossola, “International Cooperation for Benchmarking”, IRRIIS Round Table, Bonn 5 September 2007.
4. Giovanna Dondossola, “Risk Assessment in the Electric Power Industry - practices from WG members: analysis and evaluation” Cigré meeting – WG D2.22 “Treatment of Information Security in the Electric Power Utilities (EPUs)”, Swiss Grid, Zurich 7 September 2007.
5. Giovanna Dondossola “Cooperating Defence Plans for Secure Electric Power Services”, Information Day on Critical Infrastructure Protection Joint Call held Brussels, 27 September 2007
6. Jean Claude Laprie, “Modelling Interdependencies between the Electricity and Information Infrastructures”, Workshop on Critical Infrastructure Protection, organized by IFIP Working Group 10.4 Dependable Computing and Fault Tolerance, Guadeloupe, January 11-12, 2007
7. Jean Claude Laprie, Modelling Interdependencies between the Electricity and Information Infrastructures, Workshop on Critical Infrastructure as Complex Systems, (ECCS'2007), Dresde, Germany, October 5, 2007
8. Paulo Verissimo, Security Challenges of Critical Information Infrastructures: when computers meet the real world, at CyLab, Carnegie Mellon University, Pittsburgh, USA, November 2007
9. Miguel Correia, Tolerating Byzantine Behavior in Distributed Systems, at CyLab, Carnegie Mellon University, Pittsburgh, USA, December 2007
10. G. Deconinck, “Productiviteit verhogen: zijn systeemkoppelingen een doos van Pandora?,” Agoria Industrial Automation Days 2007, Sky Hall, Zaventem, May 24, 2007.
11. G. Deconinck, “Digitalisering van de procesautomatisering: waar zit de informatie in de data?,” ABB Gebruikersdag Process Automation 2007, Trivium, Etten-Leur, The Netherlands, 29 Nov 2007.
12. Felicita Di Giandomenico, “On a Framework for Modelling and Analyzing Interdependencies in Electrical Power Systems”, Workshop on Critical Infrastructure Protection, organized by IFIP Working Group 10.4 Dependable Computing and Fault Tolerance, Guadeloupe, January 11-12, 2007.
13. Susanna Donatelli, Research report presentation on “Modelling requirements for the Electrical Power System”, Workshop on Critical Infrastructure Protection, organized by IFIP Working Group 10.4 Dependable Computing and Fault Tolerance, Guadeloupe, January 11-12, 2007.
14. G.Deconinck, “ELECTA and the CRIS institute,” CRIS governing board meeting (Critical Infrastructure Institute), Reunion internacional parael intercambio de experiencias en la medicion y proteccion de area amplia, La Paz, Mexico, 27-29 Aug. 2007
15. Andrea Bobbio, "Stochastic models and methods for the safety and dependability analysis of DES", plenary talk at the conference First IFAC Workshop on Dependable Control of Discrete Systems - DCDS07, 15 June 2007
16. Paulo Veríssimo, CRUTIAL: The Blueprint of a Reference Critical Information Infrastructure Architecture, Workshop on Critical Infrastructure Protection, organized by IFIP Working Group 10.4 Dependable Computing and Fault Tolerance, January 11-12, 2007

17. Panel on "Architecting Critical Infrastructures", DSN-WADS 2007, Edinburgh 27 July 2007, participants from the CRUTIAL consortium: Andrea Bondavalli, Felicita DiGiandomenico (organizer) and Paulo Verissimo.
18. Workshop on Critical Information Infrastructures, organized in the context of the 51st IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance, Gosier, Guadeloupe, France, January 11-14 2007, Karama Kanoun, Paulo Verissimo (co-organizers)
19. P. Verissimo, Computers, meet the real world! Or Challenges of Architecting Dependable and Secure CII. Keynote speech, 13th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC'07). Melbourne-Australia, December 2007.
20. Publication of a paper presenting CRUTIAL at the LAAS magazine "La Lettre du LAAS" distributed to LAAS Partners and to general public: "Interdépendances d'infrastructures essentielles: modélisation et protection", December 2007.

6.3 Liaison with related European Projects

Members of the consortium have attended the following events organized by EU projects related to CRUTIAL. Participation to these events has provided good opportunities to keep updated with the research activities carried on in these projects and to exchange ideas about the different research directions in related areas.

An event was organized by the EU in Brussels on 15 March 2007, in conjunction with the review of the three projects IRRIIS, GRID and CRUTIAL held on the day after. It was a public event open to both the consortia of the three involved projects and to a number of invited external people. Presentations have been made on major project results by all the three projects.

1. 2nd CI2RCO CIIP conference, 7. February 2007, Rome, Italy, attended by Felicita Di Giandomenico
2. IRRIIS Workshop «Middleware Improved Technology for Interdependent Critical Infrastructures - MIT Requirements», Rome, Italy, 08.02.2007, attended by Felicita Di Giandomenico
3. 2nd GRID workshop, Vulnerabilities of power system controls: challenges and R&D needs, A Roadmap for Future Research, Paris 20 June 2007, attended by Mohamed Kaâniche
4. IRRIIS Cooperation Meeting and Public Workshop, Bonn 5-6 September 2007, attended by Giovanna Dondossola and Felicita Di Giandomenico

Outside Europe, we have close interactions with the TCIP NSF Cyber Trust Center (see Section 4.2). In particular, the IFIP WG 10.4 workshop on Critical Infrastructure Protection co-organized by CRUTIAL members, with presentations from CRUTIAL, TCIP and other teams was a good opportunity for cross fertilization and discussions about the different approaches investigated at the International level to cope with the problem of interdependencies at the levels of architecture, modelling and evaluation.

6.4 Project's technical meetings

During the second year, 3 plenary meetings have been held:

4th Technical Meeting, February 26-27, Torino, hosted by CNIT

5th Technical Meeting, May 30-31, Toulouse, hosted by LAAS;

6th Technical Meeting, October 23-24, Pisa, hosted by CNR-ISTI.

All the three meetings have been well attended by all the partners, and have been very useful forums for discussing research directions in a coordinated and cooperative manner, for showing and discussing the advancements from the previous meeting and getting feedbacks for improvements/extensions. The agenda of all the three events have also included an Executive Board Meeting session, for discussing the major issues related with the implementation of the workplan.

6.5 Dissemination through University curricula

The consortium, being made of several academic partners, has been also active towards the educational sector. In the following courses, currently running in the CRUTIAL involved University Departments, the topics of CRUTIAL are being used as use cases during classes:

- BE-KUL-H04D0: Industrial Automation and Control;
- BE-KUL-H0K03: Advanced Control and Fault Tolerance;
- IT-UNIFI-DSI: Modelling and Simulation;
- IT-UNIFI-DSI: Reliability of Processing Systems;
- IT-UNIPO- S0520: Quantitative evaluation of systems
- IT-UNITO-S8399 System’s verification
- PL-FCUL-425118: Intrusion Detection and Tolerance.

6.6 Dissemination and Exploitation activities towards industry

During the meeting held in Brussels on 15 March 2007 as a public part of the review of the three EU projects in the Electrical Power Systems sector (namely, IRRIIS, CRUTIAL and GRID), five out of the eight members of the CRUTIAL IAB were present. Presentations have been made by CRUTIAL partners on the major project results already achieved and on directions for future research (namely, on power control systems scenarios, on modelling control systems of Electrical Power System infrastructure, on the microgrid testbed, and on the CRUTIAL reference resilient architecture). A presentation was also given by the IAB member *G.* Fiorenza, Enel Distribution on the company view of needs to protect the Electricity infrastructure. Claus Kern from Siemenschaired the final discussion on CIP challenges and solutions.

This event was a relevant opportunity to present the achieved project results to the IAB members and to issue them a request for feedbacks.

6.7 Collection of Publications relative to the second year

6.7.1 Publications explicitly acknowledging the support of the CRUTIAL project.

Journals and Book Chapters:

1. F. Laroussinie and J. Sproston, “State Explosion in Almost-Sure Probabilistic Reachability”, Information Processing Letters 102(6), pp. 236-241, 2007.
2. S. Bernardi, J. Merseguer, “Performance evaluation of UML design with Stochastic Well-formed Nets”, Journal of Systems and Software, vol.80 (11): 1843-1865, November 2007.
3. Bobbio, R. Terruggia, A. Boellis, E. Ciancamerla, M. Minichino, “A Tool for Network Reliability Analysis”, Lecture Notes in Computer Science, vol. 4680, pp. 417-422, 2007, ISSN: 0302-9743.
4. Bobbio, D. Codetta-Raiteri, S. Montani, L. Portinale "Dynamic Bayesian Networks for the Reliability Analysis of Systems with Dynamic Dependencies" In "Bayesian Belief

Network: A Practical Guide to Applications", O. Pourret, P. Naïm and B. G. Marcot editors., John Wiley and Sons (TO APPEAR).

5. E.Alata, I.Alberdi, P.Owezarski, V.Nicomette, M.Kaâniche, Internet attacks monitoring with dynamic connection redirection mechanisms, Journal in Computer virology, Springer, December 2007.

Conference Proceedings

1. S. Donatelli, S. Haddad, J. Sproston, "CSLTA: an Expressive Logic for Continuous-Time Markov Chains", In M. Harchol-Balter, M. Kwiatkowska and M. Telek, editors, Proceedings of the 4th International Conference on Quantitative Evaluation of Systems (QEST'07), pp. 31-40, Endinburgh, Scotland. IEEE Computer Society Press, 2007 (Winner of the QEST'07 Best Paper Award).
2. M. Jurdzinski, F. Laroussinie, J. Sproston, "Model Checking Probabilistic Timed Automata with One or Two Clocks", In O. Grumberg and M. Huth, editors, Proceedings of the 13th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'07), Braga, Portugal. Lecture Notes in Computer Science 4424, pp. 170-184. Springer, 2007.
3. D. D'Aprile, S. Donatelli, A. Sangnier, J. Sproston, "From Time Petri Nets to Timed Automata: an Untimed Approach", In O. Grumberg and M. Huth, editors, Proceedings of the 13th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'07), Braga, Portugal. Lecture Notes in Computer Science 4424, pp. 216-230. Springer, 2007.
4. S.Bernardi, J. Merseguer, "A UML Profile for Dependability Analysis of Real Time Embedded Systems", In ACM Proc. of the 6th International Workshop on Software and Performance (WOSP07), pp. 115-124, Buenos Aires (Argentina), February, 2007.
5. L. Portinale, A. Bobbio, D. Codetta Raiteri, S. Montani, "Compiling Dynamic Fault Trees into Dynamic Bayesian Networks: the RADYBAN tool", Proceedings of the 5th Bayesian Modelling Applications Workshop (UAI-AW '07), Vancouver, Canada, July 2007. CEUR Workshop Proceedings, vol. 268, K. B. Laskey, S. M. Mahoney, J. Goldsmith editors, August 2007.
6. M. Beccuti, D. Codetta Raiteri, G. Franceschinis, S. Haddad, "A framework to design and solve Markov Decision Well-formed Net models", In Proceedings of the International Conference on Quantitative Evaluation of Systems (QEST '07), IEEE Computer Society, pp. 165-166, Edinburgh, Scotland, September 2007.
7. D. Cerotti, D. Codetta-Raiteri, S. Donatelli, C. Brasca, G. Dondossola, F. Garrone, "Representing the CRUTIAL project domain by means of UML diagrams", In Proceedings of the 2nd International Workshop on Critical Information Infrastructures Security (CRITIS '07), pp. 109-124, Malaga, Spain, October 2007.
8. Bobbio, R. Terruggia, "Binary decision diagrams in network reliability analysis", 1st IFAC Workshop on Dependable Control of Discrete Systems (DCDS'07), pp. 57-62, June 2007.
9. R. Terruggia, "Network Reliability Analysis via BDD", Int. Conference on Dependable Systems and Networks (DSN2007), pp. 303-305, Edinburgh, Scotland, June 2007.
10. Horváth, M. Telek, "Matching more than three moments with acyclic phase type distributions", Stochastic Models, vol. 23(2), pp. 167-194, 2007.
11. P. Ballarini, A. Horváth, "Compositional model checking of product-form CTMCs", In Proc. of 7th International Workshop on Automated Verification of Critical Systems (AVOCS'07), Oxford, UK, September 2007.

12. G. Dondossola, F. Garrone, J. Szanto, G. Fiorenza “Emerging information technology scenarios for the control and management of the distribution grid", in the 19th International Conference and Exhibition on Electricity Distribution, Vienna, 21-24 May 2007.
13. Anas Abou El Kalam, Yves Deswarte, Amine Baina, Mohamed Kaâniche, "Access Control for Collaborative Systems: a Web Services Based Approach", in International Conference on Web Services (ICWS 2007), IEEE Computer Society Press, Salt Lake City (UT, USA), 9-13 July 2007, pp. 1064-1071.
14. E.Alata, I.Alberdi, P.Owezarski, V.Nicomette, M.Kaâniche, Mécanisme d'observation d'attaques sur internet avec rebonds, Symposium sur la Sécurité des Technologies de l'Information et des Communications (SSTIC), Rennes (France), 31 Mai- 1 June 2007.
15. Jean-Claude Laprie, Karama Kanoun, Mohamed Kaâniche, Modelling Interdependencies between the electricity and Information Infrastructures, SAFECOMP-2007, Springer, LNCS 4680-0054, Germany, September 2007.
16. A.N.Bessani and M.Correia and J.S.Fraga and L.C.Lung. Decoupled Quorum-based Byzantine-Resilient Coordination in Open Distributed Systems. In Proceedings of the 6th IEEE International Symposium on Network Computing and Applications (NCA), pages 231-238, July 2007.
17. Alysson Neves Bessani, Miguel Correia, Henrique Moniz, Nuno Ferreira Neves, Paulo Verissimo. When 3 f +1 is not Enough: Tradeoffs for Decentralized Asynchronous Byzantine Consensus, Brief Announcements at the 21st International Symposium on Distributed Computing, Lemesos, Cyprus, September 2007.
18. Wagner Saback Dantas, Alysson Neves Bessani, Joni da Silva Fraga, Miguel Correia. Evaluating Byzantine Quorum Systems. In Proceedings of the 28th IEEE Symposium on Reliable Distributed Systems (SRDS). October 2007.
19. Manuel Mendonça, Nuno Ferreira Neves, Fuzzing Wi-Fi Drivers to Locate Security Vulnerabilities, Fast abstract at the 10th IEEE High Assurance Systems Engineering Symposium, Dallas, USA, November 2007.
20. João Antunes, Nuno Ferreira Neves, Finding Local Resource Exhaustion Vulnerabilities, Student paper at the 18th IEEE International Symposium on Software Reliability Engineering, Trollhättan, Sweden, November 2007.
21. Paulo Sousa, Alysson Neves Bessani, Miguel Correia, Nuno Ferreira Neves, Paulo Veríssimo, Resilient Intrusion Tolerance through Proactive and Reactive Recovery, Proceedings of the 13th IEEE Pacific Rim Dependable Computing conference, Melbourne, Australia, December 2007.
22. Manuel Mendonça, Nuno Ferreira Neves, Localização de Vulnerabilidades de Segurança em Gestores de Dispositivos Wi-Fi com Técnicas de Fuzzing, Actas da 3ª Conferência Nacional Sobre Segurança Informática nas Organizações, Lisboa, Portugal, October, 2007.
23. Emanuel Teixeira, João Antunes, Nuno Ferreira Neves, Avaliação de Ferramentas de Análise Estática de Código para Detecção de Vulnerabilidades1, Actas da 3ª Conferência Nacional Sobre Segurança Informática nas Organizações, Lisboa, Portugal, October, 2007.
24. Chiaradonna, S., Lollini, P., Di Giandomenico, F.: On a modelling framework for the analysis of interdependencies in electric power systems. In: IEEE/IFIP 37th Int. Conference on Dependable Systems and Networks (DSN 2007), Edinburgh, UK (2007) 185–195.
25. Romani, F., Chiaradonna, S., Di Giandomenico, F., Simoncini, L.: Simulation models and implementation of a simulator for the performability analysis of electric power

systems considering interdependencies. In: 10th IEEE High Assurance Systems Engineering Symposium (HASE'07). (2007) 305–312.

26. Bondavalli, A. Ceccarelli, L. Falai, and M. Vadursi. Foundations of measurement theory applied to the evaluation of dependability attributes. In DSN-2007 IEEE Int. Conference on Dependable Systems and Networks, June 25-28 2007.

27. Francesco Romani, Silvano Chiaradonna, Felicita Di Giandomenico, Luca Simoncini, A Simulator for Performability Analysis of Electrical Power Systems Considering Interdependencies, Fast abstract in Supplement of the International Conference on Dependable Systems and Networks (DSN), Edinburgh, UK, June 2007.

28. Alessandro Daidone, Diagnosis Framework for Complex Critical Systems/Infrastructures, in Supplement of the International Conference on Dependable Systems and Networks (DSN), Student Forum Track, Edinburgh, UK, June 2007.

29. H. Beitollahi, S.G. Miremadi, G. Deconinck, "Fault-Tolerant Earliest-Deadline-First Scheduling Algorithm in Uniprocessor Embedded System," Proc. 12th IEEE Workshop on Dependable Parallel, Distributed and Network-Centric Systems (DPDNS-2007), collocated with 21st IEEE Int. Parallel & Distributed Processing Symposium (IPDPS-2007), Long Beach, California (USA), 26-30 Mar. 2007, 6 pages.

30. T. Rigole, K. Vanthournout, G. Deconinck, "Resilience of Distributed Microgrid Control Systems to ICT Faults," Proc. 19th Int. Conf. And Exhibition on Electricity Distribution (CIRED-2007), Vienna, Austria, 21-24 May 2007, 4 pages.

31. K. De Brabandere, K. Vanthournout, J. Driesen, G. Deconinck, R. Belmans, "Control of Microgrids," Proc. 2007 IEEE Power Engineering Society nGeneral Meeting, Tampa, Florida (USA), 24-28 Jun. 2007, 7 pages.

32. G. Deconinck, T. Rigole, H. Beitollahi, R. Duan, B. Nauwelaers, E. Van Lil, J. Driesen, R. Belmans, G. Dondossola, "Robust Overlay Networks for Microgrid Control Systems," Proc. Workshop on Architecting Dependable Systems (WADS-2007), Supplemental Volume of 37th Ann. IEEE/IFIP Int. Conf. on Dependable Systems and Networks (DSN-2007), Edinburgh, Scotland (UK), 27 Jun. 2007, pp. 148-153.

33. H. Beitollahi, G. Deconinck, "Peer-to-Peer Networks applied to Power Grid," Proc. Int. Conf. on Risks and Security of Internet and Systems (CRISIS-2007), collocated with IEEE Global Information Infrastructure Symposium (GIIS-2007), Marrakech, Morocco, 2-5 Jul. 2007.

34. H. Beitollahi, G. Deconinck, "Dependability Analysis of Peer-to-Peer Networks," Proc. Int. Conf. on Risks and Security of Internet and Systems (CRISIS-2007), collocated with IEEE Global Information Infrastructure Symposium (GIIS-2007), Marrakech, Morocco, 2-5 Jul. 2007.

35. H. Beitollahi, G. Deconinck, "Overlay Networks in Dependability View," Proc. Architecture and Compilers for Embedded Systems Symp. (ACES-2007), Edegem, Belgium, 17-18 Sep. 2007; pp. 45-48.

36. R. Duan, G. Deconinck, "Prospect of MAS Coordination for Microgrids," Proc. Architecture and Compilers for Embedded Systems Symp. (ACES-2007), Edegem, Belgium, September 17-18, 2007; pp. 41-43.

6.7.2 Publications related to CRUTIAL activities but without explicit acknowledgement to CRUTIAL

Journals

1. G. Dondossola, J. Szanto, M. Masera, I.N. Fovino, "Effects of intentional threats to power substation control systems", International Journal of Critical Infrastructures (IJCI), Vol. 4, Nos. 1/2, 2008, pg. 129-143.

Conference Proceedings

1. D. Lucarella, G. Dondossola "Dalla Sicurezza della Rete Elettrica alla Sicurezza delle Infrastrutture", National Scientific Congress on Security in Complex Systems, 16-18 October 2007 (in Italian).

7 PARTNERS' PLANS FOR THE EXPLOITATION STRATEGY

The results that are expected from CRUTIAL can have a large impact on the way power generation, distribution and management will be carried out at European level. The new modelling methods and architectural solutions that will be offered are necessary for power infrastructures to cope with disrupting failures or cyber attacks. They will be to the possible extent "technology-neutral" and thus "vendor-independent", such that they can be taken-up and used by the European industry in general.

According to the current progress towards the project objectives, the following exploitable knowledge will be part of the future exploitation strategy:

a) CRUTIAL Control System Scenarios – ref. Deliverable D2 – descriptions of power control cases focused on ICT-Power interdependencies

b) CRUTIAL Modelling Framework – ref. Deliverable D16

c) CRUTIAL Testbeds – ref. Deliverable D17

d) CRUTIAL Architecture – ref. Deliverable D18

e) CRUTIAL Evaluation – ref. Deliverables D19, D20.

At the current stage most of the exploitable results are still under development. In their final version part of them will be studies/guidelines/recommendations supporting the work of interested stakeholders. Others will be meat for new tools and services to be eventually developed after the project end.

Since all the partners are academic/research organizations, direct exploitation by the partners themselves is rather limited. Therefore, the envisaged exploitation plans mainly consist in devising technological building blocks developed by the project which have strong potentialities to drive evolutions of current commercial ICT support to the electric domain and possibly trigger a new generation of ICT infrastructures for enhanced resilience and security in the electric as well as wider critical infrastructures domains. Then, strong dissemination activities will be undertaken towards relevant industry sectors, taking advantage of already established contacts by the project partners and especially through the IAB members.

In these first two years of the project lifetime, specific effort has been devoted to involving industry in evaluating the project achievements. Exploitation of CRUTIAL knowledge is also expected to be performed through the IAB members, in addition to other individual partners contacts with relevant industrial sectors and standardization bodies. Two events have provided an opportunity to meet the IAB members and to present them the achieved project results: the joint CRUTIAL/Cigré Session in Leuven on May 2006 and at the IRRIIS/CRUTIAL/GRID concerted review in Brussels on March 2007. The project deliverables produced by the end of the first year have been made available to them through the project web site and contribution for feedbacks have been explicitly asked to them, in terms of: i) comments/suggestions for improving the information exchange; ii) opinions on the project objectives, especially at what extent they meet the emerging needs of the IAB members companies; iii) critical comments on the project deliverables; iv) any other advisory issues felt useful to improve our respective benefits. The received feedbacks are reassuring on the directions explored by the project; unfortunately; details on the feedback received are reported in the Deliverable D13.

Finally CRUTIAL provided inputs and feedback to the GRID consortium about their roadmap currently under preparation and increased interactions and information exchanges with the IRRIIS consortium.

8 CONCLUSIONS AND FUTURE PLANS

This deliverable has discussed the major means and actions that the consortium has identified as effective and powerful to disseminate the project's achievements. A detailed description of the dissemination actions undertaken during the first and second year have then been included. They have mainly spanned along the following directions:

- Set up of a project web site, maintained by the coordinator with the support of the whole consortium, as a means for continuous dissemination of information about the project for the international community, as well as internally for the project participants;
- Set-up and involvement of the Industrial Advisory Board (IAB), with the aim of establishing a group of advisors who are informed about the project progress and are invited to provide their feedback during the project lifetime;
- Periodic project technical meetings, to promote internal dissemination and cross-fertilization among partners;
- Dissemination of project's results through scientific publications in the related fields of dependability, security, power system control, power system security. A significant number of publications have been already produced; the complete list relative to the first year is in Section 5.5, while that relative to the second year is in6.7;
- Dissemination through participation to Working Groups and national/international events related to dependability, security, power system control, power system security;
- Dissemination towards appropriate standardization bodies and industrial organizations, on the basis of active contacts by CRUTIAL partners;
- Dissemination towards academy and the educational sector, by using the topics of CRUTIAL as use cases during classes of several university courses currently running at the CRUTIAL involved University Departments;
- Establishment of contacts and information exchanges with related, currently active projects.

All these activities will be continued, and even reinforced, during the next year to assure prompt and wide spreading of CRUTIAL achievements towards enhancing the survivability of infrastructures for power generation and distribution and to provide guidelines to be pursued at global European level to try to uniform procedures and protocols.

With reference to dissemination at the educational level, new curricula and/or PhD courses could be related to the following CRUTIAL specific themes:

- Modelling Interdependent Infrastructures;
- Protecting Critical Infrastructures;
- Resilient Power Control Systems.

The planned thematic workshop is going to be finalized during the third year of the project. A possibility that has been discussed inside the consortium at the last Executive Meeting is to join this event with the 4th International Conference on Critical Infrastructures to be held in 2008 (still to be scheduled).

A workshop devoted to the CRUTIAL IAB is planned on the morning of 6 March 2008 (subject to confirmation).

Table 3 provides an overview of the means adopted for the dissemination of knowledge.

Planned/actual date	Type	Type of audience[2]	Countries addressed	Partner responsible/involved
Set-up in February 2006 – continuously maintained	Project web site	Research, academic, industrials, standardization bodies, public authorities, …	All the international community	CESI-R with the support of the whole consortium
Continuously during the project life	Publications	Research, academic, industrials	All the international community	ALL
Periodically during the project life	Project meetings	Project partners + IAB members (once per year)	Those of the project partners and IAB members	ALL
Continuously during the project life	Promotion events by individual partners	Research, academic, industrials, standardization bodies, public authorities, …	All the international community	ALL
Continuously during the project life	Liaison with related projects	Research, academic, industrials	EU, US	ALL
To advertise the planned thematic workshop	Posters/flyers	Research, academic, industrials	All the international community	CESI-R + ALL
Third year	Thematic workshop	Research, academic, industrials, standardization bodies, public authorities, …	Mainly EU	CESI-R + ALL

Table 3: Overview of the dissemination activities

[2] Related to dependability, security, power system control, power system security, the electricity sector at large.