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: 39 months**

Deliverable no.: D21

Title of the deliverable: Dissemination and exploitation

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

Contractual Date of Delivery to the CEC:	**31/3/2009**
Actual Date of Delivery to the CEC:	**15/05/2009**
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 Kaâniche[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:	**3.0**
Total number of pages:	**71**

Abstract:

This deliverable presents the final results and achievements concerning dissemination and exploitation in CRUTIAL. First, the dissemination actions undertaken by the CRUTIAL consortium in WP6 during the three years duration of the project are extensively described, explicitly listing the publications produced by the project. Identification of exploitable knowledge as results from the CRUTIAL and synthetic plans for their exploitation are then described. The document is largely based on the previous Deliverable D5 and Deliverable D12, on dissemination produced at the end of the first and second year respectively, and extends them by including dissemination and exploitation activities related to the third project period.

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 has been 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
24/02/09	0.0	Internal	First draft circulated by ISTI-CNR to all the partners.
09/03/09	1.0	Internal	Complete version incorporating partners comments.
11/03/09	2.0	Approved	Approved final version, with final comments incorporated.
13/05/09	3.0	Approved	Final version, with reviewers recommendations addressed

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 has been 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 has been appropriate to support the analysis and management of interdependencies and of the resulting overall operational risk.

Firstly, the project aimed 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 was to understand and master such interdependencies to avoid escalating and cascading failures that result in outages and blackouts. The focus was 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 was to find the right abstractions of the models. The aim was therefore to produce, from conceptual analysis, generic models that can be refined and instantiated. To some extent, the abstractions have been substanciated by examples taken from the electric application domain.

Secondly, the project intended 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 studied architectures address 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 was 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.

The advanced solutions devised by CRUTIAL 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. The developed designs can be deployed in different points of the critical infrastructure to protect different applications.

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 efforts undertaken during the first, second and third year are reported

in Section 5, 6 and 7, respectively, where also the collection of publications relative to the year is included (distinguished in publications explicitly acknowledging the support of CRUTIAL and those related but without acknowledgement). Plans for the exploitation strategy are briefly indicated in Section 8. Conclusions are in Section 9, where short indication of dissemination and exploitation plans still foreseen beyond the life of the project are also provided.

2 RELEVANCE OF CRUTIAL'S OBJECTIVES

Electrical energy is a *crucial* cornerstone of the European society. The *CRUTIAL* project has dealt 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 the achievements of 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)*.

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. Given the crucial relevance of electrical energy forthe European society, it is important that potential faults and the resulting interdependencies are identified, studied, modelled and assessed in detail. The CRUTIAL activity focused 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 addressed the modelling of interdependent infrastructures taking into account multiple dimensions of interdependencies, in order to be representative. The analysis and modelling of such interdependent infrastructures is also a valuable support to the definition of resilient architectural patterns of the dedicated information infrastructure.

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 of 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 included a workpackage dedicated to disseminate project achievements and to define plans to exploit them. The partners have been 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 constituted 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 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 disseminated 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 have taken 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 disseminated 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. 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 have been 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 consisted 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 represented 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 was 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. Although the partial involvement of the IAB members, such annual meetings have been held.

The CRUTIAL consortium agreed 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 Awareness	Standards committee chairs coordinate to avoid duplicative or 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.

Nine project meetings have been held during the three years, hosted by partners according to a schedule agreed among all the partners. More information on such meetings will be given when detailing the dissemination activities during the three years of the project.

3.5 Thematic workshop

With the support of the European Commission, a joint IRRIIS and CRUTIAL workshop has been organised in Brussels, 3 February 2009 to showcase the research and technology solutions pioneered by the two projects. Further details may be found in chapter 7.

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 was 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 was 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
ESTEC – European Network of SCADA Test Security Centres for Critical Energy Infrastructures	Study Funded by DG JLS under the ERN-CIP frame	01/05/2008 31/03/2009	www.estec-project.eu

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 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 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”.

[1] ACC means: Acceding and Candidate Countries

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.cesiricerca.it/testi/ricerca_di_sistema.aspx?idN=12**
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, while from 2006 to 2008 CESI RICERCA continued the RdS activity under the Contract Agreement with the Ministry of Economic Development. 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 cross fertilization.

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:

1. 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.
2. 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>).
3. 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.
4. 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
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.

11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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
19. 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.
20. 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
21. 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.
22. 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.
23. 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.

24. 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).

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

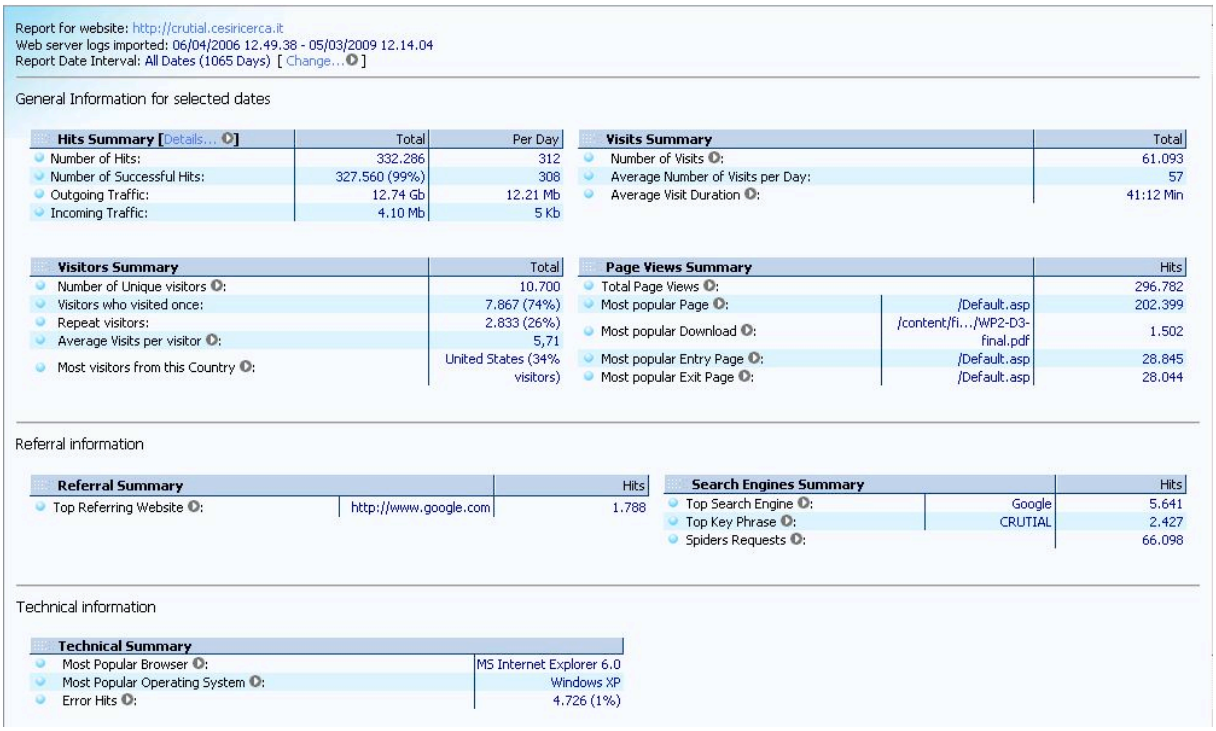
1. D. Lucarella, G. Dondossola “Dalla Sicurezza della Rete Elettrica alla Sicurezza delle Infrastrutture”, National Scientific Congress on Security in Complex Systems, 16-18 October 2007 (in Italian).

7 DISSEMINATIONS ACTIONS UNDERTAKEN DURING THE THIRD YEAR

7.1 Project Web site

Continuing from the previous two years, the project web site 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. In particular, it makes available the public deliverables to the interested community and stores documents, such as minutes of meetings, for usage internal to the consortium.

As a means of assessing the level of interest arisen by the CRUTIAL project, a statistical analysis on the project web accesses during the three years has been performed. The obtained numbers are more than positive, as can be derived from the following figures. Comparing these results with those obtained at the end of the second year (as documented in Deliverable D.13), the interest in CRUTIAL is growing, being the number of accesses to the web site kept high during the third year, with an increasing interest from a wide number of countries. Also from the point of view of documents downloads, the numbers increased a lot during the last year, and interested all the deliverables documenting the major achievements of CRUTIAL.



Report for website: http://crutial.cesiricerca.it
Web server logs imported: 06/04/2006 12.49.38 - 05/03/2009 12.14.04
Report Date Interval: All Dates (1065 Days) [Change...]

General Information for selected dates

Hits Summary [Details...]	Total	Per Day
Number of Hits:	332.286	312
Number of Successful Hits:	327.560 (99%)	308
Outgoing Traffic:	12.74 Gb	12.21 Mb
Incoming Traffic:	4.10 Mb	5 Kb

Visits Summary	Total
Number of Visits:	61.093
Average Number of Visits per Day:	57
Average Visit Duration:	41:12 Min

Visitors Summary	Total
Number of Unique visitors:	10.700
Visitors who visited once:	7.867 (74%)
Repeat visitors:	2.833 (26%)
Average Visits per visitor:	5,71
Most visitors from this Country:	United States (34% visitors)

Page Views Summary		Hits
Total Page Views:		296.782
Most popular Page:	/Default.asp	202.399
Most popular Download:	/content/fi.../WP2-D3-final.pdf	1.502
Most popular Entry Page:	/Default.asp	28.845
Most popular Exit Page:	/Default.asp	28.044

Referral information

Referral Summary		Hits
Top Referring Website:	http://www.google.com	1.788

Search Engines Summary		Hits
Top Search Engine:	Google	5.641
Top Key Phrase:	CRUTIAL	2.427
Spiders Requests:		66.098

Technical information

Technical Summary	
Most Popular Browser:	MS Internet Explorer 6.0
Most Popular Operating System:	Windows XP
Error Hits:	4.726 (1%)

Figure 1: Statistics - summary

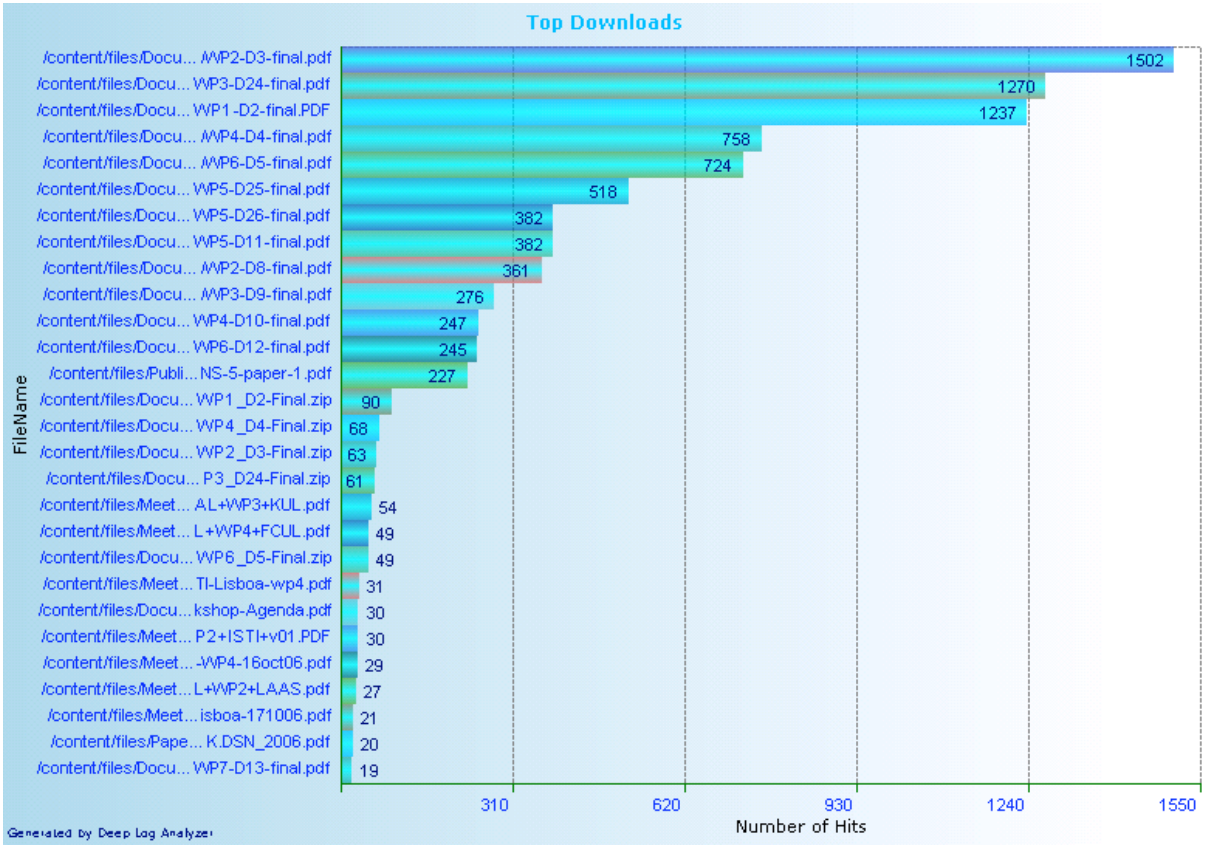


Figure 2: Statistics – Top Downloads

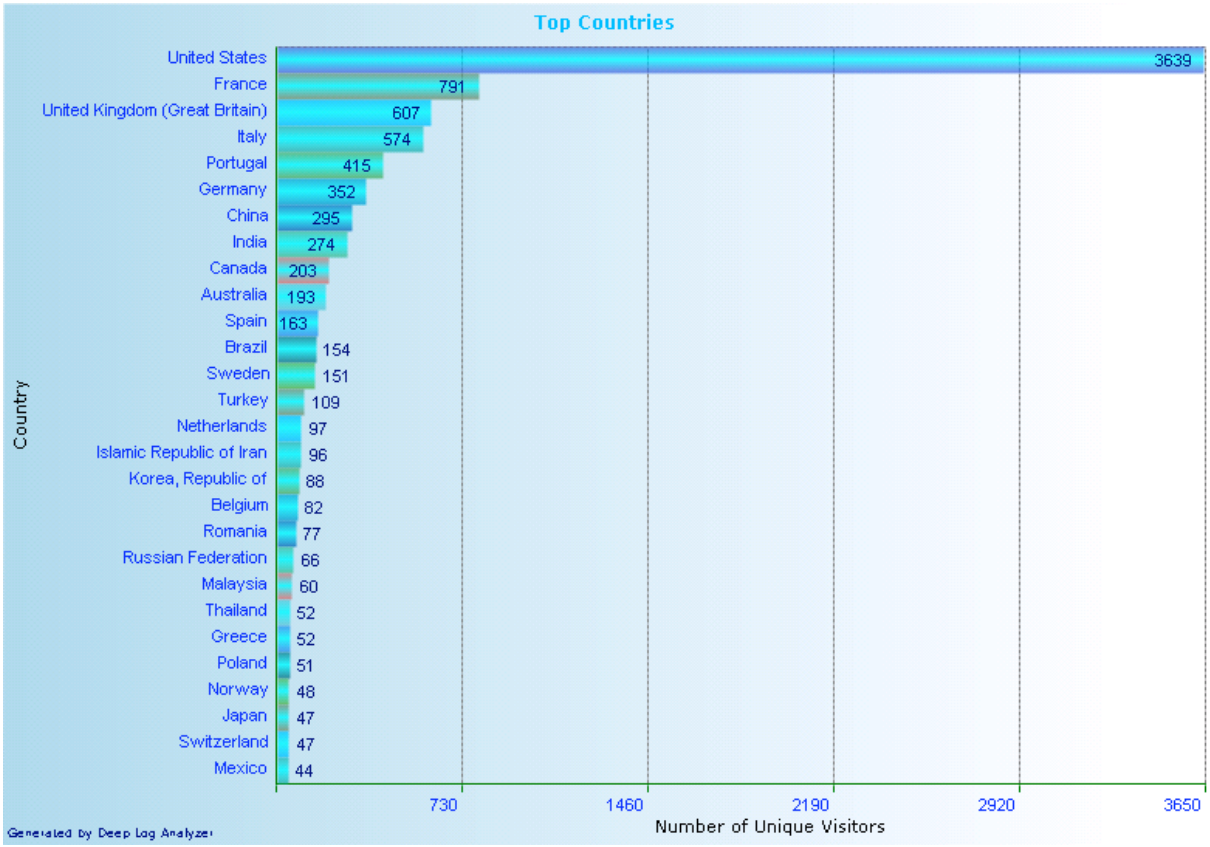
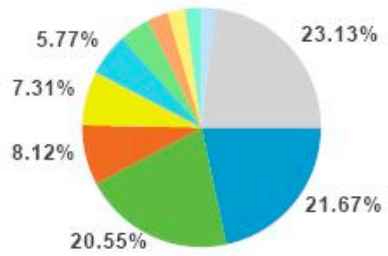


Figure 3: Top Countries

Detailed statistics on the site usage related to the last period is reported in the following Figures.

Figure 4: Geographic distribution of visiting cities.

Country/Territory	Visits	Visits
United States	563	21.67%
Italy	534	20.55%
Portugal	211	8.12%
France	190	7.31%
United Kingdom	150	5.77%
Germany	108	4.16%
Ireland	74	2.85%
Spain	61	2.35%
Bulgaria	58	2.23%
Canada	48	1.85%



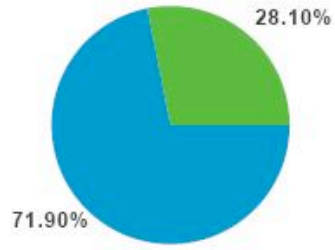
1 - 10 of 82

Figure 5: Percentage distribution of visiting countries.

Site Usage

Visits	Pages/Visit	Avg. Time on Site	% New Visits	Bounce Rate
2,601 % of Site Total: 100.00%	3.26 Site Avg: 3.26 (0.00%)	00:02:00 Site Avg: 00:02:00 (0.00%)	71.90% Site Avg: 71.86% (0.05%)	54.90% Site Avg: 54.90% (0.00%)

Visitor Type	Visits	Visits
New Visitor	1,870	71.90%
Returning Visitor	731	28.10%



1 - 2 of 2

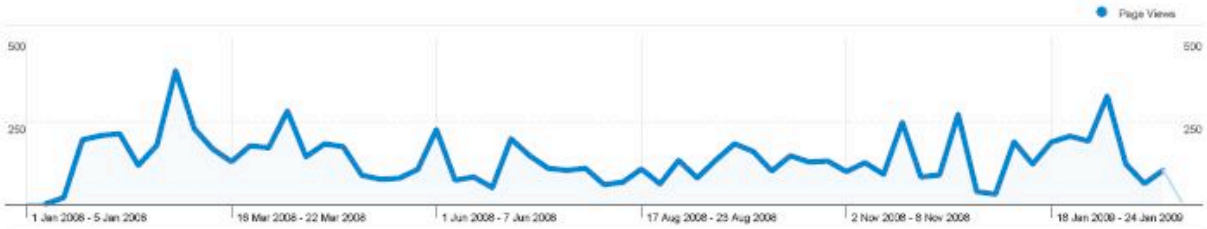
Figure 6: Traffic Sources Overview.

crutial.cesiricerca.it

Content Overview

1 Jan 2008 - 8 Mar 2009

Comparing to: Site



Pages on this site were viewed a total of 8,471 times

8,471 Page Views

6,094 Unique Views

54.85% Bounce Rate

Top Content

Pages	Page Views	% Page Views
/	2,131	25.16%
/Dissemination/DELIVERABLES-OF-THE-PROJECT.asp	980	11.57%
/default.asp	750	8.85%
/Dissemination/PUBLICATIONS.asp	538	6.35%
/Partners.asp	454	5.36%

Figure 7: Content Overview.

7.2 Presentations related to CRUTIAL and further dissemination actions

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

1) Paulo Verissimo. Future Control System Cyber Architectures: an introductory tutorial. Invited Lecturer. CYBER SECURITY FOR PROCESS CONTROL SYSTEMS SUMMER SCHOOL. Lake Geneva, Fontana, Wisconsin. June 16-20, 2008
2) Yves Deswarte, "Security Models and Policies for Critical infrastructures" (in French), Presentation on "Computer-based architectures for critical systems", SEE Club "Systèmes informatiques de confiance", Working group open meeting, January 17, Paris 2008
3) Yves Deswarte, "Access Control for Collaborative Systems: An approach based on Web services" (in French), Presentation at DISCO-SINC Seminar on "Resilience, Verification and Diagnosis of hybrid and distributed applications", LAAS-CNRS, March 25, 2008
4) Mohamed Kaaniche, Presentation of modelling related activities in CRUTIAL, Meeting with Franhaufer IESE Delegates (Components Engineering Group), LAAS-CNRS, June 18-19 2008
5) Paulo Verissimo, “Power Grid Security: past, present and future”, invited Speech at: Intelligent Power Delivery, A Logica and EDP Forum for InovGrid, EDP Auditorium, 31st March 2008, Lisbon – Portugal
6) A. Bobbio, “Stochastic modeling techniques for the dependability analysis of DES”, in 16-th Mediterranean Conference on Control and Automation MED-08, pp. 633-634 (Abstract of a Plenary Talk), June, 2008
7) F. Di Giandomenico, “A Modelling Framework for Quantitative Analysis of Interdependencies in Electrical Power Systems”, in 54th IFIP WG10.4 meeting, Alyeska, Alaska, June 2008
8) G. Dondossola, “Resilient Computing in Electric Power Utilities”, ReSIST Workshop on Best Practices in Resilient Computing, Bristol (UK) 8 February 2008
9) G. Dondossola, “Critical Utility InfrastructurAL resilience”, CIP Expert Group Meeting, Brussels (Belgium) 5 December 2008
10) M. Correia, "Critical Infrastructure Protection: the CRUTIAL Project", INTERAC 1st Plenary Workshop, University of Minho, Gualtar Campus, Braga, July 2008
11) P. Sousa, “Security and Availability through Proactive Resilience», Keynote speech at the 4th Portuguese National Conference of Informatics Security in Organizations, FCTUC, Coimbra, Portugal, October 2008
12) P. Sousa, “The Digital Wall», 1st Workshop on Cyber-Warfare of the Portuguese Republic Intelligence System SIRP, Lisbon, Portugal, September 2008
13) S. Donatelli, “Modelling at different abstraction levels: the CRUTIAL experience”, 55th IFIP WG10.4 meeting, Cortina d’Ampezzo, Italy, January 2009
14) Giovanna Dondossola, “Introduction to the CRUTIAL Project”, IRRIIS&CRUTIAL Public Workshop, Brussels, 3 February, 2009
15) Giovanna Dondossola, “The CRUTIAL testbed for macrogrid teleoperation: setup and evaluations”, IRRIIS&CRUTIAL Public Workshop, Brussels, 3 February, 2009
16) Geert Deconinck, “The CRUTIAL testbed for microgrid control: setup and Evaluations”, IRRIIS&CRUTIAL Public Workshop, Brussels, 3 February, 2009
17) Paulo Verissimo, “The CRUTIAL Information Switch: setup and evaluations”, IRRIIS&CRUTIAL Public Workshop, Brussels, 3 February, 2009
18) M. Kaâniche, The CRUTIAL modelling framework for the evaluation of Power Grid Control scenarios, IRRIIS&CRUTIAL Public Workshop, Brussels, 3 February, 2009
19) Y. Deswarte, The CRUTIAL access control: the PolyOrBAC model and its application, IRRIIS&CRUTIAL Public Workshop, Brussels, 3 February, 2009

7.3 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 strengthen the contacts with these related projects, to keep updated with the research activities carried by them and to exchange ideas about the different research directions in related areas.

- Final GRID Conference, ICT Vulnerabilities of Power Systems: A Roadmap for Future Research, Brussels (Belgium) 7 February 2008, attended by Giovanna Dondossola
- ReSIST Workshop on Best Practices in Resilient Computing, Bristol (UK) 8 February 2008 attended by Jean Claude Laprie, Karama Kanoun, Luca Simoncini, Giovanna Dondossola
- Cigré WG D2.22 Meeting, Treatment of Information Security for Electric Power Utilities (EPUs) hosted by Terna, Florence (Italy) 6-7 March 2008, attended by Giovanna Dondossola
- IRRIIS – Benchmarking activity, ENEA Meeting on CRUTIAL products/methodologies, Milan April 4 2008 attended by Giovanna Dondossola
- Final GRID Review Meeting, Brussels (Belgium) 7 April 2008, attended by Giovanna Dondossola
- Cigré WG D2.22 Phone Meeting, Treatment of Information Security for Electric Power Utilities (EPUs), 27 May 2008, attended by Giovanna Dondossola
- Cigré WG D2.22 Meeting, Treatment of Information Security for Electric Power Utilities (EPUs) hosted by RTE, Paris (France) 27 August 2008, attended by Giovanna Dondossola
- Cigré WG D2.22 Meeting, Treatment of Information Security for Electric Power Utilities (EPUs) hosted by RTE, Paris (France) 21 October 2008, attended by Giovanna Dondossola
- 2nd Meeting of the CIP Expert Group on cross-sectoral interdependencies between the ICT Sector and the Electricity Networks, Brussels (B) 5 December 2008 attended by Giovanna Dondossola
- Cigré WG D2.22 Meeting, Treatment of Information Security for Electric Power Utilities (EPUs) hosted by KEMA, Arnhem (Netherlands) 10-11 February 2009, attended by Giovanna Dondossola
- ESTEC - Visit to the CESI RICERCA Testbed by the ESTEC Team, Milan (I) 4 March 2009 attended by Giovanna Dondossola and Fabrizio Garrone
- ESTEC - Visit to the K.U.Leuven microgrid testbed by the ESTEC Team, Leuven (B) 5 March 2009 attended by Geert Deconinck and Tom Loix

7.4 Project's technical meetings

During the third year, the project convened 3 plenary meetings.

- Technical Meeting, March 4-5, 2008, hosted by CESI-R in Milan
- Technical Meeting, June 4-5, 2008, hosted by K.U.Leuven in Leuven
- Technical Meeting, October 28-29, 2008, hosted by LAAS in Toulouse.

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 meetings and getting feedbacks for improvements/extensions.

Executive Board Meetings took place in the context of the Technical Meetings, for discussing the review preparation, the review report, the dissemination issues including the final public Workshop, and for planning the reporting activity.

7.5 Dissemination through University curricula

Also during this third year, academic partners have taken the opportunity to disseminate research activities at the educational level, through courses they are involved in. Specifically, in the following courses currently running at University Departments of CRUTIAL partners, selected topics of CRUTIAL are being used as use cases during classes:

- BE-KUL-H04D0: Industrial Automation and Control
- BE-KUL--H02E1A Machinery Safety, Control Systems and Safety of Digital Systems
- 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.

7.6 Dissemination and Exploitation activities towards industry

The first event related to dissemination and exploitation activities towards industry during the third year was the workshop devoted to IAB members, which took place at CESI RICERCA premises on 6 March 2008. Three IAB members committed to attend: Tor Aalborg (Statnett), Antonio Manuel Carrapatoso (EFACEC) and Gennaro Fiorenza (ENEL Distribuzione). Unfortunately**,** Gennaro Fiorenza had to cancel his participation for unexpected problems.

Challenges and R&D needs related to ICT security were presented by Tor Aalborg, representing a Transmission System operator's view. Major tackled points were:

- TCP/IP is used everywhere and it is more vulnerable to attacks
- Off the shelf products, with little (or none) security build in, are used
- The borderline between the Enterprise and the SCADA network is changing, sharing content and resources
- No ICT security standards are covering the overall threats and vulnerabilities of the total ICT systems within utilities (IT systems, communication systems, SCADA systems, Energy Market systems etc)
- Growing interdependencies between TSO's
- National laws and regulations sometimes are contradictory
- Escalating transactions and flows among national, regional and local systems
- Forum/system for information sharing before/after break downs
- Effective ICT systems under restoration situations to minimize outage time and consequences to the community.

It can be observed that several of the needs above constitute the core motivations of the CRUTIAL project. The research achievements in the CRUTIAL WPs were then illustrated by the CRUTIAL consortium. The comments by the IAB members present were positive and encouraging on the continuation.

On 31 July 2008 there was a technical meeting between CESI RICERCA and ENEL aimed at showing the preliminary results of the Telecontrol Testbed in the CESI RICERCA laboratory. ENEL expressed full satisfaction on the work done and encouraged to continue the assessment activity of the telecontrol infrastructure. An overview about the status of the connections between the operation and maintenance ICT infrastructures has been presented. The collaboration with ENEL produced the publication of three joint papers and

posters in the context of the 19th and 20th International Conference and Exhibition on Electricity Distribution (CIRED 2007 and 2009) and in the CIRED Seminar 2008: SmartGrids for Distribution in 2008.

The second event was the Public IRRIIS and CRUTIAL Workshop, with specific reference to the Round Table organised after the Technical Sessions. Further details are in section 7.9.

7.7 Special Recognitions

The CRUTIAL consortium is extremely proud that Paulo Sousa, LaSIGE PhD researcher and member of the CRUTIAL team, has won the:

IBM Portugal 2007 Scientific Award

with the work "Security and Availability through Proactive Resilience".

http://www-05.ibm.com/pt/events/pc/premio.html

These results also inspired parts of the CRUTIAL architecture and protocols.

7.8 Collection of Publications relative to the third year

7.8.1 Publications explicitly acknowledging the support of the CRUTIAL project.

Journals

1) T. Rigole, K. Vanthournout, K. De Brabandere, G. Deconinck, “Agents Controlling the Electric Power Infrastructure,” Int. Journal of Critical Infrastructures IJCIS (Inderscience), Vol. 4, No. 1/2, 2008, pp. 96-109.
2) Alysson Neves Bessani, Paulo Sousa, Miguel Correia, Nuno Ferreira Neves, Paulo Verissimo. “The CRUTIAL way of Critical Infrastructure Protection”. IEEE Security & Privacy. Nov./Dec. 2008.
3) Alysson Neves Bessani, Miguel Correia, Joni da Silva Fraga, Lau Cheuk Lung. “Sharing Memory between Byzantine Processes using Policy-Enforced Tuple Spaces”. IEEE Transactions on Parallel and Distributed Systems, Vol. 68, Issue 9, pages 1291-1296, Elsevier. September 2008.
4) Paulo Verissimo, Nuno F. Neves, Miguel Correia. “The CRUTIAL reference critical information infrastructure architecture: a blueprint”. International Journal of System of Systems Engineering, vol. 1, n. 1/2, pp 78-95, 2008.
5) M. Gribaudo, D. Manini, B. Sericola, M.Telek. “Second order fluid models with general boundary behaviour”. In Annals of Operational Research, Volume 160, No 1, Pages 69-82, April 2008
6) P. Lollini, A. Bondavalli, F. Di Giandomenico, “A decomposition-based modeling framework for complex systems”, in IEEE Transactions on Reliability, VOL. 58, NO. 1, March 2009.
7) G. Deconinck, K. Vanthournout, “Agora. A semantic overlay network,” *Int. Journal of Critical Infrastructure IJCIS* (Inderscience), Vol. 5, Nos. 1/2, 2009, pp. 175-195.
8) A. Horvath, G. Horvath, M. Telek . A Traffic Based Decomposition of Two-class Queueing Networks with Priority Service. To appear in Computer Networks, 2009.
9) Susanna Donatelli, Serge Haddad and Jeremy Sproston. "Model Checking Timed and Stochastic Properties with CSL^{TA}". *IEEE Transactions on Software Engineering*, 2009. To appear.
10) Miguel Correia, Alysson Neves Bessani, Paulo Verissimo. “On Byzantine Generals with Alternative Plans”, Journal of Parallel and Distributed Computing, Elsevier. To appear.
11) Henrique Moniz, Nuno Ferreira Neves, Miguel Correia, Paulo Verissimo, RITAS: Services for Randomized Intrusion Tolerance, to appear in IEEE Transactions on Dependable and Secure Computing.

Book Chapters

1. G. Deconinck, K. Vanthournout, H. Beitollahi, Z. Qui, R. Duan, B. Nauwelaers, E. Van Lil, J. Driesen, R. Belmans, “A Robust Semantic Overlay Network for Microgrid Control Applications”, Architecting Dependable Systems V, R. de Lemos, F. Di Giandomenico, C. Gacek, H. Muccini, M. Vieira (eds.), Lecture Notes in Computer Science, vol. 5135, pages 101-123, Springer Verlag, 2008.
2. P. Verissimo, N. Neves, M. Correia, Y. Deswarte, A. Abou El Kalam, A. Bondavalli, A. Daidone, “The CRUTIAL Architecture for Critical Information Infrastructures”, Architecting Dependable Systems V, R. de Lemos, F. Di Giandomenico, C. Gacek, H. Muccini, M. Vieira (eds.), Lecture Notes in Computer Science, vol. 5135, pages 1-27, Springer Verlag, 2008.
3. S. Chiaradonna, F. Di Giandomenico, P. Lollini, “Evaluation of Critical Infrastructures: Challenges and Viable Approaches”, Architecting Dependable Systems V, R. de Lemos, F. Di Giandomenico, C. Gacek, H. Muccini, M. Vieira (eds.), Lecture Notes in Computer Science, vol. 5135, pages 52-77, Springer Verlag, 2008..
4. A. Daidone, S. Chiaradonna, A. Bondavalli, P. Verissimo, “Analysis of a Redundant Architecture for Critical Infrastructure Protection”, Architecting Dependable Systems V, R. de Lemos, F. Di Giandomenico, C. Gacek, H. Muccini, M. Vieira (eds.), Lecture Notes in Computer Science, vol. 5135, pages 78-100, Springer Verlag, 2008.
5. A. Bobbio, D. Codetta-Raiteri, S. Montani, L. Portinale, "Reliability Analysis of Systems with Dynamic Dependencies", In "Bayesian Networks: a practical guide to applications", O. Pourret, P. Naim and P. G. Marcot editors, pages 225-238, John Wiley and Sons, March 2008, http://www.wiley.com/go/pourret

Conference Proceedings

1. Z. Qiu, G. Deconinck, N. Gui, R. Belmans, "A multi-agent system architecture for electrical energy matching in a microgrid," Proc. 4th IEEE Young Researchers Symp. in Electrical Power Engineering (YRS-2008), Eindhoven, Belgium, The Netherlands, 7-8 Feb. 2008.
2. H. Beitollahi, G. Deconinck, "Protect Network-Based Power Grid Applications from Denial of Service Attacks," Proc. 4th IEEE Young Researchers Symp. in Electrical Power Engineering (YRS-2008), Eindhoven, Belgium, The Netherlands, 7-8 Feb. 2008.
3. H. Beitollahi, G. Deconinck, "Analyzing the Chord Peer-to-Peer Network for Power Grid Applications," Proc. 4th IEEE Young Researchers Symp. in Electrical Power Engineering (YRS-2008), Eindhoven, Belgium, The Netherlands, 7-8 Feb. 2008.
4. R. Duan, G. Deconinck, "A Prospect of Multiagent Coordination in Microgrids," Proc. 7th Power Systems Conf. (PS-2008), Clemson, SC, USA, 11-14 Mar. 2008.
5. H. Beitollahi, G. Deconinck, “An Overlay Protection Layer against Denial-of-Service Attacks,” Proc. 13th IEEE Workshop on Dependable Parallel, Distributed and Network-Centric Systems (DPDNS-2008), co-located with 22nd IEEE Int. Parallel & Distributed Processing Symposium (IPDPS-2007), Miami, Florida (USA), 14-18 Apr. 2008.
6. G. Deconinck, "An evaluation of two-way communication means for advanced metering in Flanders (Belgium)," Proc. IEEE Int. Instrumentation and Measurement Technology Conf. (I2MTC-2008), Victoria, Vancouver Island, Canada, 12-15 May 2008, pp. 900-905..
7. Beitollahi, G. Deconinck, “Analysis of Peer-to-Peer Networks from a Dependability Perspective,” *Proc. 3rd Int. Conf. on Risks and Security of Internet and Systems (CRiSIS 2008),* Tozeur, Tunisia, 28-30 Oct. 2008, pp. 101-108.
8. H. Beitollahi, G. Deconinck, “Comparing Chord, CAN, and Pastry Overlay Networks for Resistance to DoS Attacks,” *Proc. 3rd Int. Conf. on Risks and Security of Internet and Systems (CRiSIS 2008),* Tozeur, Tunisia, 28-30 Oct. 2008, pp. 261-266.
9. H. Beitollahi, G. Deconinck, “Dependable Overlay Networks,” *Proc. 14th IEEE Int. Symp. on Pacific Rim Dependable Computing (PRDC-2008)*, Taipei, Taiwan, 15-17 Dec. 2008, pp.104-108.
10. H. Beitollahi, G. Deconinck, “FOSeL: Filtering by helping an Overlay Secure Layer to Mitigate DoS Attacks,” *Proc. 7th IEEE Int. Symp. on Network Computing and Applications*

(NCA-2008), Cambridge, MA (USA), 10-12 Jul. 2008, pp. 19-28.
11. G. Deconinck, "Communication Means for Two-Way Smart Metering in Flanders," *Proc. Metering, Billing/CRM Europe 2008*, Amsterdam, The Netherlands, 22-24 Sep 2008, pp. 39.
12. Giuliana Santos Veronese, Miguel Correia, Lau Cheuk Lung and Paulo Verissimo. “Finite Memory: a Vulnerability of Intrusion-Tolerant Systems”. In Proceedings of the 7th IEEE International Symposium on Network Computing and Applications (NCA). July 2008.
13. Eduardo Alchieri, Alysson Bessani, Joni Fraga, “A Dependable Infrastructure for Cooperative Web Services Coordination”, Proceedings of the 6th IEEE International Conference on Web Services (ICWS 2008), Beijing, China. September 2008.
14. Manuel Mendonça, Nuno Ferreira Neves, “Fuzzing Wi-Fi Drivers to Locate Security Vulnerabilities”, Proceedings of the European Dependable Computing Conference (EDCC), Kaunas, Lithuania, May 2008.
15. Alysson Bessani, Eduardo Alchieri, Miguel Correia and Joni Fraga. “DepSpace: A Byzantine Fault-Tolerant Coordination Service”. Proceedings of the European Conference on Computer Systems (EuroSys 2008). April 2008.
16. Paulo Sousa, Alysson Bessani, Rafael R. Obelheiro, “The FOREVER Service for Fault/Intrusion Removal”, Proceedings of the 2nd Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS 2008). Glasgow, UK, April 2008.
17. A. Baina, A. Abou El Kalam, Y. Deswarte, M. Kaâniche, “ A collaborative access control framework for critical infrastructures”, Second Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Arlington (USA), 16-19 April 2008, pp. 189-204.
18. A. Baina, Y. Deswarte, A. Abou El Kalam, M. Kaâniche, “Access Control for Collaborative Systems: A Comparative Analysis”, Third International Conference on Risks and Security of Internet and Systems, Tozeur, Tunisia, 28-30 October 2008, Preprints (Final proceedings will be published by the IEEE Computer Society).
19. Eric Alata, Mohamed Kaâniche, Vincent Nicomette, “An Experimental Study of Dictionary Attacks", The 3rd conference on Security of Network Architectures and Information Systems (SAR/SSI 2008), Loctudy, 13-17 October 2008, France, pp. 301-315 (In French).
20. D. Cerotti, D. Codetta-Raiteri, S. Donatelli, C. Brasca, G. Dondossola, F. Garrone, “UML diagrams supporting domain specification inside the CRUTIAL project", Lecture Notes in Computer Science, vol. 5141, J. Lopez and B. M. Hämmerli editors, pages 106-123, Springer, November 2008 (Proceedings of the International Workshop on Critical Information Inftrastructures Security (CRITIS), Malaga, Spain, October 2007.
21. D. Cerotti and S. Donatelli, "Modelling Crutial Information switches with well-formed nets", presented at the International workshop on petri Nets and Distributed Systems (PNDS 2008), co-located with the 29th International Conference on petri Nets and Other Models of Concurrency, Xi'an, China, June 2008.
22. G. Dondossola, F. Garrone, J. Szanto, G. Fiorenza “A laboratory testbed for the evaluation of cyber attacks to interacting ICT infrastructures of power grid operators”, CIRED Seminar 2008: SmartGrids for Distribution, Frankfurt, Germany 23-24 June 2008.
23. M. Beccuti, D. Codetta-Raiteri, G. Franceschinis, S. Haddad, "Non deterministic Repairable Fault Trees for computing optimal repair strategy", Proceedings of the International Conference on Performance Evaluation Methodologies and Tools (VALUETOOLS), Athens, Greece, October 2008, ACM Digital Library.
24. A. Bobbio, R. Terruggia, E. Ciancamerla, M. Minichino. “Evaluating network reliability versus topology by means of BDD algorithms”. In: PSAM-9, Hong Kong, May 2008.
25. G. Bonanni, E. Ciancamerla, M. Minichino, R. Clemente, A.Iacomini, A. Scarlatti, E. Zendri, A. Bobbio, R. Terruggia. “Availability and QoS analysis of interconnected networks”. In 5th International Service Availability Symposium, ISAS 2008 Tokyo, Japan, May 19-21, 2008.
26. S. Bernardi, J. Merseguer and D.C. Petriu. "Adding Dependability Analysis capabilities to the MARTE profile". ACM/IEEE 11th International Conference on Model Driven

Engineering Languages and Systems (MoDELS'08), LNCS, September 2008.
27. M. Beccuti, G. Franceschinis, M. Kaaniche and K. Kanoun "Multi-level dependability modeling of interdependencies between the Electricity and Information Infrastructures". In Third International Workshop on Critical Information Infrastructures Security (CRITIS'08). 13-15 October 2008, Frascati, Italy, pp. 63-74. To appear in the LNCS series as CRITIS 2008 post-proceedings.
28. A. Abou El Kalam and Y. Deswarte, "Critical infrastructures security modeling, Enforcement and runtime checking", Third International Workshop on Critical Information Infrastructures Security (CRITIS'08), 13-15 October 2008, Frascati, Italy, pp. 115-128.
29. E. Alata, I. Alberdi, V. Nicomette, P. Owezarski, M. Kaâniche, "Internet Attacks Monitoring with dynamic connection redirection mechanisms", Journal in Computer Virology, Vol.4, N°2, pp.127-136, May 2008.
30. S. Chiaradonna, F. Di Giandomenico, P. Lollini, "Interdependency Analysis in Electric Power Systems", In Third International Workshop on Critical Information Infrastructures Security (CRITIS'08), 13-15 October 2008. To appear in the LNCS series as CRITIS 2008 post-proceedings.
31. G. Dondossola F. Garrone, G. Deconinck, H. Beitollahi, "Testbeds for assessing critical scenarios in Power Control Systems", Third International Workshop on Critical Information Infrastructures Security (CRITIS'08), 13-15 October 2008. To appear in the LNCS series as CRITIS 2008 post-proceedings.
32. João Antunes, Nuno Ferreira Neves, Paulo Verissimo, Detection and Prediction of Resource-Exhaustion Vulnerabilities, Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE), Seattle, USA, November 2008.
33. Eduardo Adilio Pelinson Alchieri, Alysson Neves Bessani, Joni da Silva Fraga, Fabíola Greve. Byzantine Consensus with Unknown Participants. OPODIS'08: The 12th International Conference On Principles Of DIstributed Systems. Luxor, Egypt. December 2008.
34. M. Gribaudo, D. Cerotti, A. Bobbio. Analysis of On-Off policies in sensor networks using interacting Markovian agents. In: 4-th International Workshop on Sensor Networks and Systems for Pervasive Computing - PerSens 2008, pages 300-305, Hong Kong, March 2008.
35. A. Bobbio, M.Gribaudo, M.Telek. "Analysis of large scale interacting systems by mean field method". Accepted and to appear in 5th International Conference on Quantitative Evaluation of SysTems (QEST08), St Malo, France, September 14-17, 2008.
36. S. Donatelli. "Dependent automata for the modelling of dependencies". In Third International Workshop on Critical Information Infrastructures Security (CRITIS'08), 13-15 October 2008, To appear in the LNCS as CRITIS 2008 post-proceedings.
37. S. Baarir, M. Beccuti, G. Franceschinis. New solvers for asymmetric systems in GreatSPN. In 5th International Conference on the Quantitative Evaluation of SysTems (QEST08) pages 235-236, St Malo, France,14th-17th September 2008. IEEE Computer Society Press.
38. M. Beccuti, D. Codetta-Raiteri, G. Franceschinis and S. Haddad. Parametric NdRFT for the derivation of optimal repair strategies. The International Conference on Dependable Systems and Networks (DSN 2009), PDS track. Estoril, Lisbon, Portugal June 29 - July 2 2009 (actually accepted under condition).
39. Paulo Veríssimo, Alysson Bessani, Miguel Correia, Nuno Ferreira Neves, Paulo Sousa, Designing Modular and Redundant Cyber Architectures for Process Control: Lessons Learned, Proceedings of the 42nd Hawaii International Conference for the Systems Sciences (HICSS), Waikoloa, Hawaii, January 2009.
40. M. Beccuti, G. Franceschinis, S. Donatelli, S. Chiaradonna, F. Di Giandomenico, P. Lollini, G. Dondossola, F. Garrone, "Quantification of Dependencies in Electrical and Information Infrastructures: the CRUTIAL approach", Proceedings of the Fourth International CRIS Conference on Critical Infrastructures, Sweden, April 2009.
41. G. Dondossola F. Garrone, J. Szanto, "Supportino Cyber Risk Assessment of Power Control Systems with experimental data, PCSE 2009, March 2009.

42. G. Dondossola, F. Garrone, J. Szanto, G. Fiorenza, “Assessment of Power Control Systems communications through testbed experiments”, 20th International Conference and Exhibition on Electricity Distribution (CIRED 2009), June 2009.
43. G. Dondossola, F. Garrone, J. Szanto, G. Deconinck, T. Loix, H. Beitollahi, “ICT resilience of power control systems: experimental results from the CRUTIAL testbeds”, conditionally accepted to DSN- PDS 2009 as a practical Experience Report, July 2009.

Other publications

1. Giuliana Santos Veronese, Miguel Correia, Lau Cheuk Lung. “Byzantine 2f+1 State Machine Replication with COTS Components”. Poster at European Conference on Computer Systems (EuroSys 2008). April 2008.

Some papers have been submitted for publications and are still under review process:

1. L. Portinale, A. Bobbio, D. Codetta-Raiteri, S. Montani, "Supporting Reliability Engineering in Exploiting the Power of Dynamic Bayesian Networks: the RADYBAN Tool", submitted to: International Journal on Approximate Reasoning, Elsevier.
2. A. Abou El Kalam, Y. Deswarte, A. Baina, M. Kaâniche, “PolyOrBAC: A Security Framework for Critical infrastructures”, submitted to: International Journal of Critical Infrastructure Protection (IJCIP).
3. V. Nicomette, M. Kaâniche, E. Alata, “Une analyse empirique du comportement des attaquants: expérimentations et resultats”, submitted to: Technique et Science Informatique (in French).
4. V. Nicomette, M. Kaâniche, E. Alata, “An empirical analysis of attack processes: Experiment and Results”, Submitted to: International Journal of Information Security.
5. D. Codetta-Raiteri, R. Nai, “Stochastic Activity Network models of a communication scenario inside an electrical power system”, submitted to: IEEE Transactions on Reliability in August 2008.
6. D. Codetta-Raiteri, R. Nai, “Modelling and simulating a communication scenario inside the electrical power system”, submitted to: the International Journal of Modelling and Simulation, ACTA Press, in September 2008.
7. M. Beccuti, G. Franceschinis, D. Codetta-Raiteri and S. Haddad. Non deterministic Repairable Fault Trees for computing optimal repair strategies. Submitted to: Journal on Discrete Event Dinamic Systems. Publisher Springer.
8. D. Cerotti and S. Donatelli, "Modelling CRUTIAL Information switches with well-formed nets", submitted to: the Transactions on Petri Nets and Other Models of Concurrency (ToPNoC).
9. A. Bobbio, D. Codetta-Raiteri, S. Montani, L. Portinale, "Modeling Cascading Failure Propagation via Dynamic Bayesian Networks”, submitted to: the Workshop on Dependable Control of Discrete Systems (DCDS ’09) in January 2009.

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

Journals

1. G. Dondossola, “Risk Assessment of Information and Communication Systems – Analysis of some practices and methods in the Electric Power Industry”, ELECTRA journal of the Cigré Association, Issue N°239 - August 2008.
2. Francesc Sebé, Josep Domingo Ferrer, Antoni Martínez Ballesté, Yves Deswarte, Jean-Jacques Quisquater, “Efficient Remote Data Possession Checking in Critical Information Infrastructures”, IEEE Transactions on Knowledge and Data Engineering, Vol. 20, No. 8, August 2008, pp. 1034-1038.
3. S. Montani, L. Portinale, A. Bobbio, D. Codetta Raiteri, “RADYBAN: a tool for Reliability

Analysis of Dynamic Fault Trees through Conversion into Dynamic Bayesian Networks", Reliability Engineering and System Safety, vol. 93(7), pages 922-932, S. Montani and H. Boudali editors, Elsevier, July 2008.

Conference Proceedings

1. G. Ericsson, Å. Torkilseng, G. Dondossola, A. Bartels, "Treatment of Information Security for Electric Power Utilities – Progress Report from Cigré WG D2.22". International Cigré Session 2008, Paris (France) 24-29 August 2009.
2. M. Tritschler, G. Heslinga, G. Dondossola, G. Ericsson "Information/ICT Security Risk Assessment of Operational IT Systems at Electric Power Utilities" accepted to Cigré Colloquium SC D2, October 2009.
3. Z. Qiu, G. Deconinck, N. Gui, R. Belmans, "A multi-agent system architecture for electrical energy matching in a microgrid," Proc. 4th IEEE Young Researchers Symp. in Electrical Power Engineering (YRS-2008), Eindhoven, Belgium, The Netherlands, 7-8 Feb. 2008.
4. Z. Qiu, G. Deconinck, N. Gui, R. Duan, R. Belmans, "A Market-Based MAS Framework for Microgrids," *Proc. 17th IFAC World Congress (IFAC-2008)*, Seoul, Korea, 6-11 Jul. 2008, pp. 11053-11058.
5. R. Duan, G. Deconinck, "Agent Coordination for Supply and Demand Match in Microgrids with Auction Mechanisms," Proc. Int. Conf. on Infrastructure Systems 2008 Building Networks for a Brighter Future (NGInfra - Next Generations Infrastructures Foundation and IEEE SMC), Rotterdam, The Netherlands, 10-12 Nov. 2008.

7.9 Public Workshop

A public Workshop, in conjunction with the IRRIIS project, has been held on 3 February 2009, hosted by the European Commission in Brussels. This one day workshop was attended by about forty people, including participants in the two projects CRUTIAL and IRRIIS.

The workshop started with an Introduction by Dr. Jaques Bus, Head of the Unit INFSO F5 «Trust and Security», who presented the latest EU developments on CIP. He briefly recalled the currently ongoing CIP projects with specific emphasis on potential impact of the IRRIIS and CRUTIAL projects. Then, he sketched the challenges for upcoming RTD for a Trustworthy Information Society as foreseen in the Workprogramme 09-10.

Three sessions followed, including presentations by the two projects. The first session dealt with the progresses in understanding dependencies in critical infrastructures, in terms of achievements, lessons learned and remaining problems. The second session was about testbeds for simulating dependencies in Critical Infrastructures. The last session was based on architectural solutions and working protection mechanisms for critical infrastructures. Achieved results as well as what still needs to be addressed have been discussed with reference to both CRUTIAL and IRRIIS. During the presentations, several questions have been arisen to the speakers.

A round table, chaired by Dr. Jaques Bus and participated by six industrial panellists representative of stakeholders, concluded the workshop. The Round Table was meant to hear the voice of key actors influencing, in a way or another, the quality of the power service. The Round Table panellists were invited to express their prospective on the evolution of infrastructures controlling the Electrical System, and to debate on crucial aspects in critical infrastructures, including:

1) Agreeing frameworks, platforms and tools for data collection and trusted data sharing on incidents and vulnerabilities as well as on countermeasures in Critical Infrastructures;

2) Defining agreed security metrics, and developing benchmarking and testing facilities that are openly accessible by the stakeholders and sustainable in time; this includes testbeds for CIP technology assessment, awareness raising and confidence building;
3) Agreeing upon best practices and upon certification and standardisation;
4) Developing mechanisms for attracting and involving Critical Infrastructure stakeholders with 'on the terrain' experience.

Just to mention a few of the addressed topics, Pierre Dominique Lansard, by France Telecom and member of the IRRIIS Advisory Board, stressed the importance that research projects like IRRIIS and CRUTIAL address real problems and develop applicable results. Also, he underlined the need to increase the consideration of the Telecomunication Infrastructures in the arena of Critical Information Infrastructure Protection.
Claus Kern, by Siemens AG and member of the CRUTIAL Advisory Board, who already chaired the panel session at the previous workshop in March 2007, congratulated with the progress done and encouraged the research teams to continue in promoting ICT advanced technologies for the power industry.
Enzo Maria Tieghi, by Vision Automation, underlined the need to increase the awareness of cyber security risks within the Corporate and Business Units of the Power Utilities.

Their views on relevant issues on which the research community is called to contribute, although very shortly presented, have reinforced the needs to progress in this challenging field. At the same time, they represented the right audience at the workshop to which the achievements of the two projects are directed to, and they constitute a formidable vehicle of dissemination of the projects activities inside their organizations.

8 PLANS FOR THE EXPLOITATION OF CRUTIAL RESULTS

The scientific and technological objectives of CRUTIAL have been motivated by the need of technological progresses to allow commercial Intelligent Electronic Devices to be effectively deployed for the protection of citizens against cyber threats to electric power management and control systems. A well-founded know-how needs to be built inside the industrial power sector to allow all the involved stakeholders to achieve their service objectives without compromising the resilience properties of the logical and physical assets that support the electric power provision: this requirement is particularly stringent since the recent introduction of a competitive electric power market. The SCADA systems, to which the process control of utility infrastructures is demanded, were classically not designed to be widely distributed and remotely accessed, let alone be open. They grew-up standalone, closed, not having security in mind.

In this context, CRUTIAL has contributed with the development 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. Therefore, results achieved by 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, architectural solutions and testbeds developed in the context of CRUTIAL have been designed to enhance the capability of power infrastructures in coping with disrupting failures or cyber attacks. They have been developed 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. Many different stakeholders are expected to benefit from the CRUTIAL results, including:

- Electric power utilities, transmission and distribution operators, industrial manufacturers, SCADA suppliers, system integrators, etc.;
- The electricity sector at large (including regulators), by knowing where vulnerabilities

arise, and how serious they can be and, consequently, the directions in which regulations and standards in the electricity sector have to evolve for coping with adequate protections of advanced control infrastructures;

- Public authorities, by better coping with the risks associated to interdependent infrastructures;
- European citizens and 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.

However, since all the CRUTIAL partners are academic/research organizations, exploitation plans mainly consisted in:

- devising technological building blocks, 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;
- making these results available to potentially interested industrial organizations, e.g. SCADA manufacturers;
- opening to new areas of research and acquiring new areas of expertise;
- participating in technical fora to which project achievements are of interest;
- exploiting links with industrial and regulatory organizations;
- attracting more students on project's related topics.

At the end of its 39 months duration, the project has developed a number of exploitable knowledges, which constitute rather mature results to be exploitable by several stakeholders in the electric power sector.

They mainly consist in:

1) Control System Scenarios
2) Modelling and Evaluation Framework
3) Dependent Automata, Formalism and Tool
4) EPS Simulator: EPSyS
5) Architectural Solutions and CIS
6) PolyOrBAC Access Control Framework
7) FOSEL Security Layer
8) Telecontrol Testbed and Experimental Data
9) Microgrid Testbed
10) Honeypot Implementations and Attack Data
11) AJECT: Attack Injection Tool

These exploitable knowledges are fully detailed in the project deliverables. Most of these results can be regarded as prototype tools and services to be evaluated by interested stakeholders and eventually developed after the project end.

8.1 CRUTIAL Exploitable knowledge

This Section gives an overview of the CRUTIAL exploitable knowledge. A table is defined for each of the exploitable results, where:

- the column " Reference Documents" indicates the project deliverables where the result is described;
- the column "Sector(s) of Application" indicates possible application area and related stakeholders interested in the product of knowledge;
- the column "Maturity Level" indicates the level of maturity of the product of knowledge, in view of its exploitation by interested stakeholders;
- the column "Additionally Required Technology" indicates additionally required technology development and exploitation by the project members themselves or by other researchers/developers in order to be able to present the CRUTIAL modules both separately and as an integrated value proposition to the industry sector to be utilised for increased infrastructure security;
- the column "Dissemination Level Already Reached" is related to the dissemination of the product of knowledge, in addition to project deliverables.

1 Control System Scenarios

Exploitable Knowledge	Reference Documents	Sector(s) of application	Maturity Level	Additionally Required Technology (for commercial use)	Dissemination level already reached
Control system scenarios	Deliverable D2	Electric Power Utilities, Operators and Authorities, industrial manufactures, SCADA suppliers, system integrators, public institutions	Representative set of microgrid and telecontrol scenarios, ready to evaluate the impact of failing ICT and power components on the electrical applications	Instantiation of the details to the different stakeholders (system operators, suppliers, market participants, regulators, communication providers, etc)	Published in scientific papers Presented at several technical forums – both industrial and academic Presented to IAB members

What is the exploitable result? (functionality, purpose, innovation etc.):

A control system scenario defines a reference structure and behaviour of a power grid portion, of the monitoring and control network, with Intelligent Electronic Devices at different levels of the power control hierarchy (Control Centre level, Station level, Bay level, Process level), the structure of the management information networks and their functional relationships with the process network, together with the different threats that may threaten the operation of the power system services. A representative set of scenarios has been described both for the case of centralized control and teleoperation as for the more forward looking case of decentralized or distributed microgrid applications.
These scenarios have proved to be useful for supporting different types of activities including:

1) the validation of power control applications under different threat scenarios, 2) the elaboration of dependability and security evaluation models taking into account different interdependency scenarios, 3) the illustration of new access control policies and mechanisms in operational contexts involving multiple organizations with different security policies and requirements, 4) the validation of architectural solutions increasing the resilience of power system communications to cyber threats., 5) the implementation of attacks to control functions.

Which partner(s) is/are involved in the exploitation? Please shortly describe their role and activities:

CESI-R and the University of Leuven have mainly worked on the definition of scenarios that cover emerging themes involving ICT for Power System bulk generation, transmission and distribution infrastructures including:

- the security of the remote supervision and control functions for grid and generation operators
- the impact of attacks in emergency conditions
- the possible breaches caused by the interconnections between the corporate and the process networks
- the possible problems related to the ICT Systems' remote maintenance.

These partners are mainly going to exploit these results internally to their organizations in CRUTIAL follow-up research activities whose validation also involves industrial stakeholders. However, other academic partners are going to use these control scenarios for further studies in understanding and analysing interdependencies, and at level of academic courses related with dependability/security assessment of critical, complex systems.

How might the result be exploited? (products, processes, projects) - directly (spin offs etc.) or indirectly (licensing) – on an individual basis or as a consortium/group of partners:

This result is not going to become an actual product, but a reference structure and behaviour of a power grid and related management information networks and devices, together with the different threats that may threaten the operation of the power system services control network and devices.

Both the CRUTIAL scenarios and the methodology adopted for their description constitute a practical result directly usable by the power utilities. For instance at the management level they are exploitable for conducting a scenario-based Risk Assessment, focusing on dependencies of the power services from the ICT infrastructures supporting their control, management and maintenance. The CRUTIAL scenarios are also very useful to the community working on the modeling and assessment of interdependencies in critical information infrastructures.

Are there any technical and economic market considerations? (commercial and technical thresholds etc):

None

Are there any obstacles identified which might prove to be barriers to commercialisation?

-the existence or development of similar or competing technologies / solution elsewhere

-third party rights (e.g. patents belonging to competitors), standards,…

-analysis of any (potential) non-technical obstacles:

One difficulty in the exploitation of CRUTIAL scenarios is related to the fact that interdependency issues necessarily involve competences distributed in several units of the Power Utilities' organisation: for instance automation operation is managed by a unit which is separate from the unit in charge of data network management; again the control infrastructure security is normally managed apart from power system security.

At institutional level, formal relationships with Electric Power Authorities and Regulators should

be set-up to foster the consideration of ICT-Power interdependencies.
Is there any form of non-commercial use or impact, relating e.g. to the development of new standards or policies? The availability of scenarios such as those developed in CRUTIAL supports the adoption of a risk based approach to the analysis of power system security during power system planning and operation. Consequently the CRUTIAL scenarios influence the development of security standards and policies for power control infrastructures.
Is there any further additional research and development work, including need for further collaboration? The defined scenarios constitute highly representative scenarios, both for the case of centralized control and teleoperation, as well as for the more forward looking case of decentralized or distributed microgrid applications. They have completely fulfilled the needs of the CRUTIAL project related to both interdependencies analysis and risk assessment, and are still very useful in further studies related to these topics. So, no needs for further collaboration, although extensions of the scenarios and possible comparisons with others in related CI areas would be interesting follow on.
Have any commercial contacts been taken, demonstrations given to potential licensees and/or investors and any comments received? *(market requirements, potential etc.)*: A subset of the CRUTIAL scenarios have been implemented in the CRUTIAL testbeds and deployed in the demonstrators of CRUTIAL architectural solutions. Demonstrations of the testbeds to industrial stakeholders have been performed in the last phase of the project and will continue after the project end. Many appreciations have been collected from the demonstrations and suggestions on enhancing the experiment coverage to intrusions cases have been received.

2 Modelling and Evaluation Framework

Exploitable Knowledge	Reference Documents	Sector(s) of application	Maturity Level	Additionally Required Technology (for commercial use)	Dissemination level already reached
Modelling and Evaluation Framework	D.8, D.11, D.16, D.25, D.19	The electricity sector at large (operators, SCADA manufactures, and also including regulators) Public authorities of Interdependent critical infrastructures	Methodologies and models available (both conceptual and implemented models, through commercially available tool) Ad-hoc, academic level, analysis tool developed Extension to DrawNet tool	Engineering by professional developers Integration in industry-level evaluation environment	Published in scientific papers Presented at several technical forums – both industrial and academic Presented to IAB members

What is the exploitable result? (functionality, purpose, innovation etc.):

The interdependencies between infrastructures have been analysed in the CRUTIAL Modelling and Evaluation Framework by means of models at different abstraction levels: i) *from a very abstract view* expressing the essence of the typical phenomena due to the presence of interdependencies, ii) *to an intermediate detail level* representing in a rather abstract way the structure of the infrastructures, in some scenarios of interest, iii) *to a quite detailed level* where the system components and their interactions are investigated at a finer grain, considering elementary events occurring at the level of the components and analyzing their impact at the system level. These three levels are exploitable in isolation or in a synergic combination, according to the specific needs of the analysis at hand. The peculiarities of the interdependencies-related failures, of the involved electric and cyber components and the assessment of the impact of such failures on the dependability and security of the services delivered by the electricity power systems have not only generated a new methodological approach to the interdependencies analysis, but also triggered extensions to/generation of analysis tools (such as the simulator EPSyS and extension to the DRAWNET tool) which, although developed at academic level, could be a basis for the development of commercial tools at industry level. Moreover, in CRUTIAL the methodology has been applied to scenarios derived from power systems application contexts. However, the proposed methodology can be applied to other application fields provided that the failure models and the interdependencies scenarios are adapted to the corresponding contexts.

Which partner(s) is/are involved in the exploitation? Please shortly describe their role and activities:

CNIT, CNR-ISTI and LAAS-CNRS have mainly worked on the definition of the modeling framework and they are going to exploit it in their organizations, in terms of:

- new studies, mainly development/refinements of methodologies, techniques and tools for dependability and security assessment of critical, complex systems and infrastructures;
- new material for academic courses, master and PhD theses.

CESI-R is going to exploit the CRUTIAL model-based evaluation framework for the impact analysis of control scenarios implemented in the telecontrol testbed.
The CRUTIAL Consortium as a whole will contribute to the dissemination of the results related to the interdependencies modelling framework through the presentation of CRUTIAL results and achievement in different forums and conferences.

How might the result be exploited? (products, processes, projects) - directly (spin offs etc.) or indirectly (licensing) – on an individual basis or as a consortium/group of partners:

The project has developed new methodologies and models for interdependencies analysis and assessment in Electric Power systems. Both conceptual and implemented models, (through commercially available tool, such as Mobius) have been provided, which constitute a solid basis for the realization of innovative tools for the analysis of EPS systems where both the electrical grid and the control information infrastructure are accounted for. Of course, a proper engineering phase is necessary, as well as the integration in industry-level evaluation environments for this evaluation framework to be of practical usage for the security planning and operation processes within Electric Power Utilities..

Are there any technical and economic market considerations? (commercial and technical thresholds etc):

From the feedbacks received during the presentation of these results at technical forums and conferences including both industrial and academic audience, there is a need on the market of advanced tools for interdependencies analysis which account for both aspects pertaining to the transmission/distribution grid and to the information control infrastructure and related SCADA devices, as well as accounting for different kinds of threats, both accidental and malicious ones. CRUTIAL has developed results which provide important initial contributions in this direction, although effort is still necessary to yield them into market-level technologies.

Are there any obstacles identified which might prove to be barriers to commercialisation?

-the existence or development of similar or competing technologies / solution elsewhere

-third party rights (e.g. patents belonging to competitors), standards,…

-analysis of any (potential) non-technical obstacles:

Consolidated tools supporting the analysis of power system security are currently used by Power Utilities that would need to be re-designed in consideration of new threats and dependencies. However, the tool re-design also implies to review the utility organisation in terms of resources, competences and internal processes.

At institutional level it is difficult to get consensus among stakeholders on relevant indices and criteria.

Is there any form of non-commercial use or impact, relating e.g. to the development of new standards or policies?

The CRUTIAL Modelling and Evaluation Framework supports the Risk Assessment activity during power system planning and operation. Its adoption indirectly contributes to the development of security standards and policies for power control infrastructures.

Is there any further additional research and development work, including need for further collaboration? The three approaches to interdependencies analysis developed in CRUTIAL are exploitable in isolation or in a synergic combination, according to the specific needs of the analysis at hand. A demonstration of synergic usage has been provided in deliverable D19. Although project objectives on interdependencies analysis have been fully accomplished, further cooperation among involved partners to exploit other synergic usages of the developed approaches would be advisable and is partly planned as follow on of the CRUTIAL activities. Further investigations would be also needed to confirm the applicability of the proposed modelling framework to other application areas.
Have any commercial contacts been taken, demonstrations given to potential licensees and/or investors and any comments receive? (market requirements, potential etc.): At this stage, the presentation of the CRUTIAL modelling framework has been done in technical conferences and working groups. This effort could lead in a longer term to the establishment of industrial contacts for further exploitation into commercial products.

3 Dependent Automata, Formalism and Tool

Exploitable Knowledge	Reference Documents	Sector(s) of application	Maturity Level	Additionally Required Technology (for commercial use)	Dissemination level already reached
Dependent Automata Formalism and Associated Tool	D.8, D.16	Company and research institutions that want to describe dependencies in a formal manner	Formalism has been defined, implemented and put at work on examples of dependencies between the ICT and the electrical infrastructure Academic tool developed, highly portable (Java based) and based on the multiformalism open tool DrawNET	Engineering by professional developers Integration in industry-level software, like the UML tool, possibly as a behavioural diagram like statecharts	Published in scientific papers Presented in a few technical forums Presented to IAB members
What is the exploitable result? (functionality, purpose, innovation etc.): Dependent Automata has been introduced as a formal settings to study (inter)dependencies.					

While interacting state models (like statechart) are centered on the autonomous behaviour of the components, and interaction among them is considered as a special case, in dependent automata dependency of one automaton from the other ones is the normal behaviour, and autonomous behaviour a special case.

Dependent automata model the critical infrastructure as a set of automata, one per infrastructure, focussing the attention of the modeller on the dependencies between automata. Dependent Automata have an associated tool that allows a system to be defined in terms of components, and algorithms have been defined, and developed inside the tool, for the composition of two or more automata into a single system.

Which partner(s) is/are involved in the exploitation? Please shortly describe their role and activities:

Dependent Automata have been developed by CNIT, but their application to the ICT and power infrastructure has been done in collaboration with LAAS-CNRS and CESI, that have defined the qualitative models of the infrastructures on which Dependent Automata have been applied.

How might the result be exploited? (products, processes, projects) - directly (spin offs etc.) or indirectly (licensing) – on an individual basis or as a consortium/group of partners:

Dependent Automata and its analysis tool are now available to the whole research and development community. Although some additional engineering effort is still required, the technique could be already used in teaching (to disseminate knowledge on critical infrastructure behaviour) and in specific applications.

Since the formalism has been implemented on the DrawNET platform, that allows a formalism to inherit definitions and solutions from other formalisms, it is also envisionable that Dependent Automata can be profiled on specific application fields

Are there any technical and economic market considerations? (commercial and technical thresholds etc):

As far as we know, there is no formalism in which dependencies is easier to describe than independencies. This is the centre of the exploitation of dependent automata. The precise formalization of interdependencies may find interesting applications in many application fields, and industrial areas. Altough, at the present state of the art, only the interdependencies between EI and II have been analysed, the availability of the related DrawNet analysis tool favours the exploitation of Dependent Automata in other interdependent infrastructures.

Is there any form of non-commercial use or impact, relating e.g. to the development of new standards or policies?

It could be of interest to see whether, if a profile of UML for critical infrastructures would be defined in the future, dependent automata can be a basic building block for the compositional definition of interdependent critical infrastructures.

Is there any further additional research and development work, including need for further collaboration?

The Dependent Automata approach has been specifically developed for the CRUTIAL project. Further research is needed to extend the capabilities of the technique. A work that could not be performed was to apply dependent automata to critical infrastructures other than ICT and power (due to lack of case study in the literature). New areas of application need to be explored.

Have any commercial contacts been taken, demonstrations given to potential licensees and/or investors and any comments receive? (market requirements, potential etc.):

At this stage, the presentation of Dependent Automata has mainly addressed the academic environment.

4 EPS Simulator: EPSyS

Exploitable Knowledge	Reference Documents	Sector(s) of application	Maturity Level	Additionally Required Technology (for commercial use)	Dissemination level already reached
EPS Simulator: EPSyS	Deliverables D.8; D.11, D.16 and D.25	The electrical sector at large, with interest in analysis of interdependiency, explicitely accounting for the electrical grid and the control information infrastructure	Stochastic models of EPS systems are defined A first complete, academic-level version of the tool is available	Additional effort to engineer the tool according to industrial-level standards	Published in scientific papers Presented at few technical forums

What is the exploitable result? (functionality, purpose, innovation etc.):

EPSyS is an ad-hoc simulator developed for Electric Power Systems, which allows to analyse interdependencies between the electric grid and the information based control system. It is based on a stochastic behaviour of the involved infrastructures and related failure models. It allows to quantitatively assess the reciprocal impact of malfunctions experienced by the involved infrastructures, through the definition of performability related indicators, well representative of user-perceived quality of service of the EPS system (such as measures of black-out).

A first version of the simulator is available and used in a few artificial scenarios to acquire a better knowledge of the impact of interdependencies through properly identified metrics. It helped to refine the generic SAN (Stochastic Activity Network) models populating the evaluation framework. Acually, the development of the two methods to assess the consequences of failures in power systems are also very useful to be exploited for cross validation among the methods themselves.

The development of EPSyS has been held highly modular so, if needed, it is possible to interface domain-specific simulators with some modules, in order to achieve a more realistic simulation.

Which partner(s) is/are involved in the exploitation? Please shortly describe their role and activities:

The development of the EPSyS tool has been performed by CNR-ISTI. In its current version, the tool is available to be exploited mainly by this partner, both at reasearch level and at academic level, namely in academic courses related to evaluation of complex, critical

infrastructures, master and PhD theses.
How might the result be exploited? (products, processes, projects) - directly (spin offs etc.) or indirectly (licensing) – on an individual basis or as a consortium/group of partners: As an academic tool, EPSyS is exploitable as a means to support feasibility studies in the modeling and assessment of interdependency analyses, and to this purpose it is available on demand. To become a tool with industrial impact, it is necessary to engineer it by professional developers and integrate it in industry-level evaluation environment.
Are there any technical and economic market considerations? (*commercial and technical thresholds etc)*: From the feedbacks received during the presentation of CRUTIAL results at technical forums and conferences including both industrial and academic audience, there is a need on the market of advanced tools for interdependencies analysis which account for both aspects pertaining to the transmission/distribution grid and to the information control infrastructure and related SCADA devices, as well as accounting for different kinds of threats, both accidental and malicious ones. Through its approach in accounting for the involved EPS subsystems and their interactions in an explicit way, EPSyS contributes to the understanding of interdependencies relations and effects. *Are there any obstacles identified which might prove to be barriers to commercialisation?* *-the existence or development of similar or competing technologies / solution elsewhere* *-third party rights (e.g. patents belonging to competitors), standards,…* *-analysis of any (potential) non-technical obstacles*: Not applicable
Is there any form of non-commercial use or impact, relating e.g. to the development of new standards or policies? No specific obstable has been identified. Many, high-professional simulators are currently in use in the electric sector. However4, they have not been specifically developed to address interdependencies between the electric grid and the control infrastructure. Currently, other research projects (mainly, the European project IRRIIS) are investigating on similar topics.
Is there any further additional research and development work, including need for further collaboration? In the last period of the project, CNR-ISTI has suspended the development of EPSyS in favour of the modeling environment based on SAN models and Mobius. However, there are plans for enhancing the current functionalities of EPSyS, also in view of possible next involvement in new studies in the electrical domain.
Have any commercial contacts been taken, demonstrations given to potential licensees and/or investors and any comments received? (market requirements, potential etc.): None at the moment.

5 Architectural solutions and the CRUTIAL Information Switch (CIS)

Exploitable Knowledge	Reference Documents	Sector(s) of application	Maturity Level	Additionally Required Technology (for commercial use)	Dissemination level already reached
Architectural solutions and the CRUTIAL Information Switch (CIS)	D.4, D.10, D.18	Electric power utilities Transmission and distribution operators Industrial manufacturers SCADA suppliers, system integrators, etc Other sectors of critical infrastructures	Generic, engineering-friendly solutions available "Phase 1" - migration from perimeter-defense to defense-in-depth paradigm (e.g. WAN-of-LANs+CIS) "Phase 2" - achieving incremental resilience up to very high levels in seamless way (CIS hierarchy; automatic and adaptive techniques and algorithms)	Industry-proof software development, compatible with existing applications	Published in scientific papers Presented and demonstrated at several technical forums – both industrial and academic Presented to IAB members

What is the exploitable result? (functionality, purpose, innovation etc.):

From the point of view of the **architectural solutions** and protection mechanisms, the developed designs can be deployed by industrial partners to protect their critical information infrastructures. Although we focused on the computer systems behind electrical utility infrastructures as an example, the overall architecture is generic and may come to be useful as a reference model for modern critical information infrastructures. The developed techniques and algorithms aim at achieving resilience to faults and attacks in an automatic and adaptive way. In particular, the intrusion-tolerant CRUTIAL Information Switch (CIS) achieves control of the command and information flow at the network boundaries, and secures a set of necessary system-level properties, like a sophisticated firewall combined with intrusion detectors, connected by distributed protocols. Several CIS designs were

proposed, trading off deployment costs with resilience, in order to support various criticality levels of the equipments that have to be protected. The most dependable CIS solution is intrusion-tolerant, prevents resource exhaustion to provide perpetual operation, and is resilient against assumption coverage uncertainty, ensuring survivability. Additionally, several DoS-resistant designs have been proposed.

Which partner(s) is/are involved in the exploitation? Please shortly describe their role and activities:

FCUL, LAAS_CNRS, CNR-ISTI and KUL have mainly worked on the architectural solutions and they are going to exploit them in their organizations, in terms of:

- new studies, mainly development/refinements of architectural paradigms, mechanisms and protocols for dependability and security assurance in critical, complex systems and infrastructures;
- new material for academic courses, master and PhD theses.

CESI-R is going to evaluate the CRUTIAL protocols and mechanisms within the WAN-of-LANs of the Telecontrol Testbed.

How might the result be exploited? (products, processes, projects) - directly (spin offs etc.) or indirectly (licensing) – on an individual basis or as a consortium/group of partners:

The project has developed new architectural paradigms, protocols and mechanisms to protect critical information infrastructures. The proposed architecture organizes the critical infrastructure as WAN-LANs, and uses protection devices at the LAN boundaries to control the command flow in and out of the LANs. Over the project duration, several kinds of protection devices were studied and developed, ranging from ready available firewalls, to more evolved security devices like the CIS. Therefore, organizations involved in critical infrastructure operation can use the architectural guidelines of CRUTIAL to set up their networks, and select appropriate protection solutions from the market to increase the level of resilience. Regarding the more advanced protection mechanisms that were designed, these can be taken by stakeholders to be incorporated in new commercial products. The protocols and mechanisms were described in detail in several documents, and proof of concept prototypes were produced, which will be demonstrated to interested parties.

Are there any technical and economic market considerations? (commercial and technical thresholds etc):

From the feedbacks received during the presentation of these results at technical forums (both industrial and academic), there is a need on the market of advanced architectural solutions and mechanisms to enhance the information control infrastructure and related SCADA devices. The reliance on standard and application independent technologies should facilitate the commercial exploitation of the CRUTIAL results and their use in the European economy and market of critical information protection.

Are there any obstacles identified which might prove to be barriers to commercialisation?

-the existence or development of similar or competing technologies / solution elsewhere

-third party rights (e.g. patents belonging to competitors), standards,…

-analysis of any (potential) non-technical obstacles:

The exploitation of CRUTIAL architectural results is made difficult by the distribution of the competences and responsibilities within several units of the Power Utilities' organisation.

The fragmentation of responsibilities also add cpmplexity to the institutional level that has to govern control centres belonging to different jurisdictions.

Is there any form of non-commercial use or impact, relating e.g. to the development of new standards or policies? The CRUTIAL architecture is strictly related to the development of the sector standards for the security of power control systems and their communications.
Is there any further additional research and development work, including need for further collaboration? As regards to the CIS designs, more development and implementation would be necessary in order to transform the current demonstrators in commercial products. In particular, further integration between the proposed mechanisms and the operating system needs to be performed, and a complete security analysis of the resulting system has to be carried out. More progress has also to be done in the support sub-systems for diversity generation and management.
Have any commercial contacts been taken, demonstrations given to potential licensees and/or investors and any comments received? (market requirements, potential etc.): Presentations of the CRUTIAL architecture and mechanisms have been done in several forums where potential investors were present, and in some cases, quite positive feedback was received. We have scheduled other demonstrations for the future with more stakeholders, where we expect to be able to augment the feedback received until now.

6 PolyOrBAC access control framework and mechanisms

Exploitable Knowledge	**Reference Documents**	**Sector(s) of application**	**Maturity Level**	**Additionally Required Technology (for commercial use)**	**Dissemination level already reached**
PolyOrBAC access control framework and mechanisms	D.4, D.10, D.18	Electric power utilities Transmission and distribution operators Industrial manufacturers SCADA suppliers, system integrators, etc More general critical information application sectors	Generic, engineering-friendly solutions available The developed concepts are mature enough and can be exploited in other development processes and products	Industry-proof software development, compatible with existing applications	Published in scientific papers Presented and demonstrated at several technical forums – both industrial and academic Presented to IAB members

What is the exploitable result? (functionality, purpose, innovation etc.):

In the context of CRUTIAL, a new security access control framework has been developed, called PolyOrBAC, that is aimed at offering each organization involved in a critical information infrastructure the capacity of collaborating with the other ones, while maintaining a control on its resources and on its internal security policy. PolyOrBAC has been designed to be generic and independent of a specific application area. It relies on two widely accepted models and technologies: 1) OrBAC for the modelling of the security policy of individual organisations, and 2) Web services for implementing the secure interactions between organizations.

Which partner(s) is/are involved in the exploitation? Please shortly describe their role and activities:

LAAS_CNRS has mainly worked on the PolyOrBAC framework and they are going to exploit them in their organizations, in terms of:

- new studies, mainly development/refinements of architectural paradigms, mechanisms and protocols for dependability and security assurance in critical, complex systems and infrastructures;
- new material for academic courses, master and PhD theses.

How might the result be exploited? (products, processes, projects) - directly (spin offs etc.) or indirectly (licensing) – on an individual basis or as a consortium/group of partners:

The proposed PolyOrBAC framework has been designed to be generic and independent of a specific application area. The dissemination of the proposed framework and its potential wide exploitation in new commercial products, processes and projects will be facilitated by the fact that it relies on two mature and widely accepted models and technologies. In particular, the use of the web services technology to implement the interactions between organizations is an attractive advantage that should facilitate the adoption of PolyORBAC by other communities and the development of commercial tools implementing the proposed framework.

PolyOrBAC can be used in the context of critical infrastructure protection for different purposes: 1) to define and specify intra-organizational and inter-organizational access policies, 2) to specify and deploy e-contracts that can be agreed between critical information infrastructures of collaborating organizations, and 3) to enforce access control policies, and detect possible use violations and abuses through runtime checking.

Are there any technical and economic market considerations? (commercial and technical thresholds etc):

From the feedbacks received during the presentation of these results at technical forums (both industrial and academic), there is a need on the market of advanced architectural solutions and mechanisms to enhance the information control infrastructure and related SCADA devices. The reliance on standard and application independent technologies should facilitate the commercial exploitation of the CRUTIAL results and their use in the European economy and market of critical information protection.

Are there any obstacles identified which might prove to be barriers to commercialisation?

-the existence or development of similar or competing technologies / solution elsewhere

-third party rights (e.g. patents belonging to competitors), standards,…

-analysis of any (potential) non-technical obstacles:

The main difficulty in the exploitation of CRUTIAL PolyOrBAC is in the need to involve several units of the Power Utilities' organisation and several jurisdictions external to it.

Is there any form of non-commercial use or impact, relating e.g. to the development of new standards or policies? PolyOrBAC is strictly related to the development of standard access control policies.
Is there any further additional research and development work, including need for further collaboration? Further development would be needed to extend the results obtained in the context of CRUTIAL by taking into account availability and integrity requirements. Further progress is also needed to integrate multiple criticality levels and the corresponding information flow control.
Have any commercial contacts been taken, demonstrations given to potential licensees and/or investors and any comments received? (market requirements, potential etc.): The demonstrator developed in the context of CRUTIAL and presented at the final review meeting will be used in future presentations of the PolyOrBAC framework to the industrial community. This should facilitate the establishment of future contacts with industrial partners and potential investors for the exploitation of PolyOrBAC into commercial products.

7 Architectural solutions: the FOSEL Security Layer

Exploitable Knowledge	Reference Documents	Sector(s) of application	Maturity Level	Additionally Required Technology (for commercial use)	Dissemination level already reached
Architectural solutions: FOSEL security layer	D.18	Electric power utilities Transmission and distribution operators Industrial manufacturers SCADA suppliers, system integrators, etc	Generic proof-of-concept solution available	Industry-proof software development, compatible with existing applications	Published in scientific papers Presented at several technical forums – both industrial and academic Presented to IAB members
What is the exploitable result? (functionality, purpose, innovation etc.): Within the set of CRUTIAL **architectural solutions** and protection mechanisms, the *Fosel* approach combines the self-healing principles of a communication overlay network with filtering based on IP-source and with random dropping of messages to increase the resilience of the communication network among application sites against denial-of-service attacks.					

Which partner(s) is/are involved in the exploitation? Please shortly describe their role and activities:

KUL has mainly worked on the Fosel architectural solution and is going to exploit it in her organizations, in terms of:

- new studies and research projects, mainly development/refinements of architectural paradigms, mechanisms and protocols for dependability and security assurance in critical, complex systems and infrastructures;
- new material for academic courses, master and PhD theses.

How might the result be exploited? (products, processes, projects) - directly (spin offs etc.) or indirectly (licensing) – on an individual basis or as a consortium/group of partners:

The project has developed new architectural paradigms, protocols and mechanisms to protect critical information infrastructures. These ideas or concepts can be taken up by industry for integration in industrial communication products.

Are there any technical and economic market considerations? (commercial and technical thresholds etc):

From the feedbacks received during the presentation of these results at technical fora (both industrial and academic), there is a need on the market of advanced architectural solutions and mechanisms to enhance the information control infrastructure and related SCADA devices. Specifically, if industrial communication is going to rely more on open communication environments, which are vulnerable to denial-of-service attacks, the need for Fosel-like solutions to increase DoS-resilience will grow.

Are there any obstacles identified which might prove to be barriers to commercialisation?

-the existence or development of similar or competing technologies / solution elsewhere

-third party rights (e.g. patents belonging to competitors), standards,…

-analysis of any (potential) non-technical obstacles:

No specific obstacles have been identified.

Is there any form of non-commercial use or impact, relating e.g. to the development of new standards or policies?

Not applicable

Is there any further additional research and development work, including need for further collaboration?

Additional design and testing is required to withstand a broader set of faults and attacks.

Have any commercial contacts been taken, demonstrations given to potential licensees and/or investors and any comments received? (market requirements, potential etc.):

None

8 Telecontrol Testbed and Experimental Data

Exploitable Knowledge	Reference Documents	Sector(s) of application	Maturity Level	Additionally Required Technology (for commercial use)	Dissemination level already reached
Telecontrol Testbed and Experimental data	D.24, D.9, D.17	Electric Power Utilities and operators SCADA manufactures Electric Power Authorities	Reference (although scaled-down) control infrastructure Evaluation Framework Results from testbed experiments available as useful source of data, sharable among organizations in the CI field	Additional scenarios of interest and their specific control algorithms need to be developed	Published in scientific papers Presented and demonstrated at several technical forums – both industrial and academic Presented to IAB members

What is the exploitable result? (functionality, purpose, innovation etc.):

The **Telecontrol Testbed** represents an embryonic platform for assessing the resilience of grid control systems to cyber threats. It consists of substations automation networks, interconnected to control centre networks, in turn interconnected to corporate intra-nets and external centres.

The Evaluation Framework consists of repeatable experiments and metrics.

A set of experimental results on the effectiveness of Denial of Service experiments on secure IEC 60870-5-104 communications are made available to the interested communities (industrial, technical and scientific).

Which partner(s) is/are involved in the exploitation? Please shortly describe their role and activities:

CESI-R has worked on the set-up and operation of the Telecontrol Testbed and he is going to exploit the testbed in future research activities. Already planned extensions to the CRUTIAL platform address i) the resilience testing of commercial products, ii) additional threat scenarios and iii) cyber-power impact analysis.

How might the result be exploited? (products, processes, projects) - directly (spin offs etc.) or indirectly (licensing) – on an individual basis or as a consortium/group of partners:

The **Telecontrol Testbed** may evolve in the future research directions: i) the resilience capabilities of advanced architectural solutions developed by the CRUTIAL partners can be evaluated in extended testbeds implementing critical scenarios of smart grids control and wide area defense systems ii) measurements from the Telecontrol Testebd and quantitative evaluation from the CRUTIAL Modeling framework could be further developed in an experimental/model-based risk assessment framework.

At industrial level, the **telecontrol testbed** has the potential of:

- improving the security know-how in power control systems
- increasing the security awareness in real time operation
- reducing the security gap between the short term operation planning (off-line analysis) and real time operation (on-line analysis)
- mitigating the vulnerabilities of the standard protocols (e.g. TCP/IP, IEC 60870-6, IEC 60870-5-104, IEC 61850, IPSEC) by testing advanced technological solutions
- testing resilience of SCADA and automation system infrastructures
- joint training of involved actors (TSOs, DSOs, GENCOs, Telecom and Internet Service Providers, etc.)
- supporting the development of cyber security standards, guidelines and practices for industrial usage (e.g. NERC, IEEE, NIST, ISA, IEC).

Are there any technical and economic market considerations? (*commercial and technical thresholds etc)*:

From the feedbacks received during the demonstrations of the Telecontrol Testbed clearly resulted that the testbed scale greatly influences both the technical complexity and the costs associated to the experimental activity. Necessarily focused objectives has to be defined to make the experimental activity technically manageable and financially reasonable.

Are there any obstacles identified which might prove to be barriers to commercialisation?

-the existence or development of similar or competing technologies / solution elsewhere

-third party rights (e.g. patents belonging to competitors), standards,…

-analysis of any (potential) non-technical obstacles:

At the technical level, the fragmentation of responsibilities within Electric Power Utilities organisations makes the exploitation diffucult.

The financial charge of investments, that are finalised to increasing the quality of a public power service regulated by a competitive power market, has to be addressed at institutional level.

Is there any form of non-commercial use or impact, relating e.g. to the development of new standards or policies?

The Telecontrol Testbed results have a direct impact on the development of sector standards as the Part 7 of the IEC 62351 on the security through network and system management.

Is there any further additional research and development work, including need for further collaboration?

Additional scenarios, control scheme and related threats may be implemented as extensions to the CRUTIAL Telecontrol Testbed.

Have any commercial contacts been taken, demonstrations given to potential licensees and/or investors and any comments received? (market requirements, potential etc.):

In the last phase of the project, the telecontrol testbed exploitation capabilities have been demonstrated to industries and ongoing European initiatives in the frame of the establishment of the European Reference Network for Critical Infrastructure Protection (ERN-CIP). The Telecontrol Testbed has been evaluated by the ESTEC project conducting a feasibility study on an European Network of SCADA Test Security Centres for Critical Energy Infrastructures.

9 Microgrid Testbed

Exploitable Knowledge	Reference Documents	Sector(s) of application	Maturity Level	Additionally Required Technology (for commercial use)	Dissemination level already reached
Microgrid Testbed	D.24, D.9, D.17	The electricity sector at large (operators, SCADA manufactures, and also including regulators) Public authorities	Reference (although partial) platforms, partly sharable among researchers for rapid prototyping of solutions (microgrid testbed) Results from testbeds available as useful source of data, sharable among organizations in the CI field	Specific additional algorithms and scenarios of interest need to be developed	Published in scientific papers Presented at several technical forums – both industrial and academic Presented to IAB members

What is the exploitable result? (functionality, purpose, innovation etc.):

The **microgrid testbed** developed in CRUTIAL consists of 4 power electronic invertors that are connected both electrically (via a power network) and logically (via a communication network). It is programmable from a dedicated extension to the Matlab environment. This microgrid testbed is also a platform for other researchers that elaborate different electrical or control aspects of distributed energy sources.

Which partner(s) is/are involved in the exploitation? Please shortly describe their role and activities:

KUL has worked on the set-up and operation of the microgrid testbed and is going to exploit it in her organization, in terms of usage in other R&D projects, PhD works and demonstration of the concepts to industry. Among other projects, the testbed will pay a pivotal role in a next (regional) project on smart grids. At an industrial level, the microgrid testbed allows rapid prototyping of different distributed control algorithms to investigate their vulnerabilities with respect to ICT faults and to evaluate solutions against such threats.

How might the result be exploited? (products, processes, projects) - directly (spin offs etc.) or indirectly (licensing) – on an individual basis or as a consortium/group of partners:

The microgrid testbed remains at the university premises, but is available for projects, research work and demonstration.

Are there any technical and economic market considerations? (*commercial and technical thresholds etc)*: From the feedbacks received during the presentation of these results at technical fora (both industrial and academic), the value of the test platform lies in its proof of concept, but several additional steps need to be performed before it can be taken up by industry …. *Are there any obstacles identified which might prove to be barriers to commercialisation?* *-the existence or development of similar or competing technologies / solution elsewhere* *-third party rights (e.g. patents belonging to competitors), standards,…* *-analysis of any (potential) non-technical obstacles*: No specific obstacles have been identified.
Is there any form of non-commercial use or impact, relating e.g. to the development of new standards or policies? Not applicable
Is there any further additional research and development work, including need for further collaboration? The microgrid testbed will be used in other research projects at European level (Vsync, Seesgen-ICT, …) and regional level (Smart Grids in Flanders).
Have any commercial contacts been taken, demonstrations given to potential licensees and/or investors and any comments received? (market requirements, potential etc.): None

10 Honeypot Implementations and Attack Data

Exploitable Knowledge	Reference Documents	Sector(s) of application	Maturity Level	Additionally Required Technology (for commercial use)	Dissemination level already reached
Honeypot and Attack data	D.26, D.20	All sectors where the information infrastructure could be a potential target of malicious attacks Public authorities	Ready to deploy high-interaction honeypot architecture Real attack data collected from the field	More vulnerabilities need to be implemented in the honeypot to provide an interesting target for the attackers, together with corresponding monitoring mechanisms	Published in scientific papers Presented at several technical forums – both industrial and academic
What is the exploitable result? (functionality, purpose, innovation etc.): Honeypots have become in the recent years a popular mechanism for collecting real data about attacks targetting systems and services deployed on the Internet. Traditional honeypot implementations generally offer a low level of interaction with the attackers and do not					

implement real functional services that can be used by the attacker to control the target victim. In CRUTIAL, a high-interaction honeypot has been developed that can be used to monitor the activities carried out by potential attackers once they manage to get the control of a target machine and try to progress in the intrusion process to get additional privileges. Such honeypot is well suited to analyse the activities performed manually by human beings in addition to automatic attacks. The implementation developed and deployed in the context of CRUTIAL has been designed to monitor attacks performed through the SSH service. The data captured include: 1) the logins and passwords tried by the attackers to break into the system, 2) all the commands and the keystrokes of the attackers on their terminals, and 3) the communication traffic going though the honeypot over the network. The data collected during the project allowed to analyze the activities performed by the attackers and to elaborate statistical models characterizing the probability distribution of the times between attacks, which is useful for quantitative evaluation models of security. Both the honeypot architecture and the collected data will be made available to the community on demand. This will allow the deployment of the CRUTIAL honeypot architecture at other locations to consolidate and extend the preliminary results about malicious activities observed in the course of the project. Aso, by making the data available, other types of models and analyses can be performed by other groups outside the CRUTIAL consortium.

Besides the high-interaction honeypot architecture and data, a low interaction honeypot architecture has been deployed that has been tuned to emulate a set of services and protocols used in SCADA systems (ModBus, DNP3 , IEC 60870-6, 60870-5-104 and 61850, etc.). Both the SCADA honeypot implementation and the collected data will be also made available to the community.

Which partner(s) is/are involved in the exploitation? Please shortly describe their role and activities:

The development and deployment of the honeypots has been performed by LAAS. He will be the main partner involved in the exploitation of the corresponding results by: i) providing assistance for the deployment of the honeypots at other locations, and ii) providing the attack data collected during the project for further analyses and modelling studies.

How might the result be exploited? (products, processes, projects) - directly (spin offs etc.) or indirectly (licensing) – on an individual basis or as a consortium/group of partners:

The honeypot implementation and the collected attack data will be made available to the community on demand.

Are there any technical and economic market considerations? (*commercial and technical thresholds etc)*:

The honeypots and the data will be made available for education purposes and also to improve our global knowledge about malicious attacks on the Internet. Commercial use of these results is not really appropriate in this context,

Are there any obstacles identified which might prove to be barriers to commercialisation?

-the existence or development of similar or competing technologies / solution elsewhere

-third party rights (e.g. patents belonging to competitors), standards,…

-analysis of any (potential) non-technical obstacles:

Not applicable

Is there any form of non-commercial use or impact, relating e.g. to the development of new standards or policies?

Not applicable

Is there any further additional research and development work, including need for further collaboration? Both the high interaction honeypot and the SCADA honeypot implementations offer a limited set of services and vulnerabilities that can be exploited by the attackers. Extensions are needed to enhance the capabilities offered by the current implementations.
Have any commercial contacts been taken, demonstrations given to potential licensees and/or investors and any comments received? (market requirements, potential etc.): Not Applicable

11 Attack Injection Tool (AJECT)

Exploitable Knowledge	Reference Documents	Sector(s) of application	Maturity Level	Additionally Required Technology (for commercial use)	Dissemination level already reached
Attack Injection Tool (AJECT)	D.26, D.20	All sectors where software could be a potential target of malicious attacks	Ready to deploy vulnerability discovery architecture and tool Field experience with network servers for DNS, IMAP, and POP3	Additional effort to make the tool completely stable, and development of user manuals	Published in scientific papers Presented at several technical forums – both industrial and academic Some interactions with software developers

What is the exploitable result? (functionality, purpose, innovation etc.):

The increasing reliance society is putting on networked computer systems, in particular in critical information infrastructures, has made security become a system attribute of the utmost importance. This is even more relevant as new threats and forms of attack are constantly being revealed, compromising the security of systems. In CRUTIAL a new attack injection methodology has been developed for the automatic discovery and removal of vulnerabilities in software components. The proposed methodology, implemented in the AJECT tool, follows an approach similar to hackers and security analysts to discover vulnerabilities in network connected servers. AJECT uses a specification of the server's communication protocol and predefined test case generation algorithms to automatically generate a large number of attacks. Then, while it injects these attacks through the network, it monitors the execution of the server in the target system and the responses returned to the clients. The observation of an unexpected behaviour suggests the presence of a vulnerability that was triggered by some particular attack (or group of attacks).
To assess the usefulness of this approach, several attack injection campaigns were performed with available DNS, POP and IMAP servers. The results show that AJECT could effectively be used to locate vulnerabilities, even on well-known servers tested throughout the years.

Which partner(s) is/are involved in the exploitation? Please shortly describe their role and activities:

The development of the attack injection methodology and the AJECT tool has been performed by FCUL. FCUL will be the main partner involved in the exploitation of the corresponding results by:

- making the tool available to interested parties;
- making further studies and developments to the methodology and tool;

including the methods and results in advance level courses in the area of security (master and Ph.D. level).

How might the result be exploited? (products, processes, projects) - directly (spin offs etc.) or indirectly (licensing) – on an individual basis or as a consortium/group of partners:

The attack injection methodology that was proposed in CRUTIAL can be implemented and used to extend vulnerability detection products offered on the market, in order to increase their capabilities for server protocol specification, automatic test generation, and target system monitoring. The AJECT tool will be eventually available to the research community and software programmers, to support the development of software projects especially in the testing phases, contributing to the implementation of more secure systems.

Are there any technical and economic market considerations? (*commercial and technical thresholds etc)*:

The advancements in software development have provided an increasing number of useful applications with an ever improving functionality. These enhancements, however, are achieved in most cases with larger and more complex projects, which require the coordination of several teams of people. Third party software, such as COTS components, is frequently utilized to speedup development, even though in many cases it is poorly documented and supported. In the background, the ever present tradeoff between thorough testing and time to deployment affects the quality of the software. These factors, allied to the current development and testing methodologies, have proven to be inadequate and insufficient to construct dependable software. Therefore, there is currently a need for methodologies and tools that can help programmers develop secure software, with minimal numbers of vulnerabilities.

Are there any obstacles identified which might prove to be barriers to commercialisation?

-the existence or development of similar or competing technologies / solution elsewhere

-third party rights (e.g. patents belonging to competitors), standards,…

-analysis of any (potential) non-technical obstacles:

Not applicable

Is there any form of non-commercial use or impact, relating e.g. to the development of new standards or policies?

Not applicable

Is there any further additional research and development work, including need for further collaboration?

FCUL is currently exploring several ways to extend the methodology and tool, in order to make it require less setup work and improve the detection capabilities for certain classes of vulnerabilities.

Have any commercial contacts been taken, demonstrations given to potential licensees and/or investors and any comments received? (market requirements, potential etc.):

The AJECT tool has been used to test several commercial products available on the market, mainly DSN and email software servers. Our contacts with the developers, after the discovery of new vulnerabilities, have been extremely positive in most cases. In particular, some of the developers have expressed their desire to employ the tool to test the software, since it provides a more complete testing coverage than the other products they are using.

8.2 Applicability to other application areas and contexts

The investigations conducted by CRUTIAL on interdependencies analyses and architectural solutions have potentialities to be helpful in other critical infrastructures as well. The proposed methodology for understanding and analysing interdependencies could be applied to other application fields (e.g., for gas or water or fuel distribution networks), provided that the failure models and the interdependencies scenarios are adapted to the corresponding contexts.

The generic architectural solutions, as well as the access control model and mechanisms, are exploitable as reference model for achieving high resilience to faults and attacks in modern critical information infrastructures, for a wide range of application fields sharing the WAN-of-LANs architectural paradigm.

The testbeds and results obtained from them are undoubtedly an important source of data to compare different CI criticalities and products. Initiatives to set up International Cooperation for Benchmarking, such as the one activated by the IRRIIS project to contribute to developing a methodology for the comparison of different products for CIP and lay the foundation for the creation of an International Network of Test Centres, would greatly benefit from this CRUTIAL activity.

Of course, more direct contacts with related CIP areas are necessary to better understand the cross-fertilization level with CRUTIAL. The consortium, as a whole or by individual partners, is willing to exploit/reinforce/extend the expertise acquired working in CRUTIAL in upcoming new projects in related areas.

For example, in a new to be started regional (Flemish) project on smart grids, K.U.Leuven will consider both electricity and gas networks - on the one hand this provides an additional degree of freedom for the control applications, but on the other hand introduces dependencies on an additional infrastructure. Both the gas and the electrical grid are supervised from an ICT architecture and are hence vulnerable to attacks and faults.

9 CONCLUSIONS

This deliverable has discussed the major means and actions that the CRUTIAL consortium has identified as effective and powerful to disseminate the project's achievements and 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. A detailed description of the dissemination actions undertaken during the project lifetime have then been included, that 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 were informed about the project progress and 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. The lists of publications, grouped per year, have been included in this deliverable. The production of joint publications involving two or more partners has been considerable, especially during the last year of the project;
- 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;
- Dissemination through workshops, both directed to IAB members (May 2006 and March 2008) and open to the community (IRRIIS & CRUTIAL Public Workshops, March 2007 and February 2009);
- Establishment of contacts and information exchanges with related, currently active projects.

In addition, plans for the exploitation of CRUTIAL results have been presented, focusing on a number of exploitable knowledges. They constitute rather mature results that can be regarded as methodologies, prototype tools and services to be evaluated by interested stakeholders and eventually exploited in industrial products to be developed after the project end.

Although the project reached its end with complete fulfillment of the objectives stated in the contract, some activities related to refinements/extension of CRUTIAL studies are still ongoing at some partners' site, and they are planned to be completed notwithstanding the end of the project. These additional results would certainly bring added value to the project itself.

Moreover, given the acquired expertise, new curricula and/or PhD courses could be anyway started in the future at the educational level by the academic partners, related to the following CRUTIAL specific themes:

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

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

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
3 February 2009	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.