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.: D22

Title of the deliverable: Final Activity Report

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

Period covered: from 01/01/2006 to 31/03/2009
Date of preparation: 10/03/2009
Project coordinator organisation name: CESI RICERCA
Project coordinator name: Giovanna Dondossola
Author(s): Giovanna Dondossola[1] (Editor); Geert Deconinck[5]; Felicita Di Giandomenico[3]; Susanna Donatelli[6]; 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: PP
Version: 002
Total number of pages: 37

Abstract:

During the 39 months of the project running the consortium shared a lot of knowledge and worked constructively towards its global objectives. The collaborative research allowed to produce an extensive set of exploitable knowledges briefly described in this deliverable. Full details about these achievements and their exploitations may be found in the final deliverables of the CRUTIAL project.

Keyword list: critical control system scenarios, interdependency modelling and evaluation, testbed platforms, resilient architectures, dissemination, exploitation.

DOCUMENT HISTORY

Date	Version	Status	Comments
10/03/2009	001	Int	First draft with requests of contributions to WP leaders
16/03/2009	002	Apr	Consolidated version
30/04/2009	003	Int	Reviewers' recommendations addressed
14/05/2009	004	Apr	Final comments integrated

Table of Contents

EXECUTIVE SUMMARY

The CRUTIAL project addressed new networked ICT (Information and Communication Technologies) systems for the management of the electric power grid, in which artefacts controlling the physical process of electricity transportation need to be connected with information infrastructures, through corporate networks (intranets), which are in turn connected to the Internet.

CRUTIAL' s innovative approach resided in modelling interdependent infrastructures taking into account the multiple dimensions of interdependencies, and attempting at casting them into new architectural patterns, resilient to both accidental failures and malicious attacks.

Firstly, the project aimed to develop comprehensive modelling approaches, supported by measurement based experiments, to analyse 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. Effort was focused 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.

Secondly, the project investigated distributed architectures dedicated to the control and management of the power grid, in the perspective of improving the capability of analysing critical scenarios and designing dependable interconnected power control systems. The architectures addressed requirements coming from the needs of flexible electric power services, characterized by dispersed energy resources, on-demand control and generation-load variations 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 project integrated leading industrial persons and academic researchers from three critically important, but presently only weakly connected disciplines: i) electrical power generation, transportation and distribution ii) resilient (self-healing) distributed and secure real-time systems and iii) modelling of complex systems. All three disciplines are necessary in order to pursue a separately unachievable objective. During the 39 months of the project running the consortium shared a lot of knowledge and worked constructively towards its global objectives. The collaborative research allowed to produce an extensive set of exploitable knowledges that may be grouped as follows:

a) CRUTIAL Control System Scenarios

b) CRUTIAL Modelling Framework

c) CRUTIAL Testbeds

d) CRUTIAL Architecture

e) CRUTIAL Evaluation.

The following sections summarise the exploitable knowledges resulting from the CRUTIAL project. An additional chapter provides an integrated view of the project achievements positioning those results according to each other relationships. Further details about the exploitation of the CRUTIAL results may be found in the Deliverable D21 – Dissemination and Exploitation.

I. CONTROL SYSTEM SCENARIOS

During the first year of the project, considerable effort has been devoted to collect information from existing systems, their renewal plans and emerging evolutions from the scientific and technical literature. Considering the largeness (and complexity) of the amount of systems and devices falling under the umbrella of power system control, the acquired knowledge was certainly partial and the power system picture derived had the only ambition to support the identification of sample control scenarios highlighting critical interdependencies among power and ICT (Information, Communication Technology) services.

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 wide set of control system scenarios has been identified and described as sample classes of behaviours available for further exploration [1]. The control system scenarios derived from the analysis of current and new systems exemplify some defence actions which are/will be undertaken, automatically or manually, in different conditions of the power system (i.e. normal, alert, emergency, in extremis, restorative), by focussing on the interactions of control/communication systems belonging to different stakeholders, the integration between the Process and Corporate Networks, the evolution of ICT maintenance, the new control schemes of distributed generation resources.

The reference control system scenarios cover both centralised schemes for teleoperations and distributed schemes for (secondary and tertiary) distributed generation control, and provide concrete evidence of the following emerging, ICT related themes:

- Communication security in the remote supervision and control functions for grid operators and generation companies
- Impact of attacks during power operators interactions in emergency conditions
- Possible breaches caused by the integration of operation and maintenance functions
- Possible problems related to the remote ICT maintenance for grid operators
- Security of interactions among Transmission and Generation ICT systems
- Impact of Denial of Service (DoS) attacks and wrong information on distributed control schemes.

The concept of control system scenarios revealed a valuable support for starting the discussion on the interdependencies of Electrical Infrastructures (EI) and Information Infrastructures (II) during the first two years of the project running. In the following years, the control system scenarios have been used as reference cases for i) the analysis of interdependencies between EI and II through the validation of the qualitative models ii) the development and validation of the testbeds iii) the demonstration of the CRUTIAL Information Switch functionality iv) the evaluation of web services for Access Control v) the validation of the quantitative Modelling Framework.

II. INTERDEPENDENCIES MODELLING

A critical review of the state of knowledge related to the dependability modelling in a large context, considering the challenges underlying the interdependencies modelling in critical infrastructures has been provided by the CRUTIAL project before starting the development of the modelling framework [2].

The CRUTIAL Modelling Framework followed two main complementary objectives:

1. The development of qualitative models describing the typical failures that are characteristic of interdependent infrastructures, i.e., cascading, escalating and common cause failures. Here the infrastructures are modelled globally without explicitly describing their components behaviours
2. The development of more detailed models of the infrastructures allowing the evaluation of quantitative measures of dependability and performance, taking into account the internal structure of the infrastructures and the behaviour of their components resulting from the occurrence of electrical and ICT failures and recoveries.

In CRUTIAL the interdependencies between infrastructures have been investigated 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 components level and analyzing their impact at the system level.

Accordingly, the proposed framework [3] is based on a hierarchical modelling approach that accommodates the composition of different types of models and formalisms, including generalized stochastic Petri nets (GSPNs), fault trees (FT), Stochastic Well formed Nets (SWN), and Stochastic Activity Networks (SAN). Each of these formalisms brings particular benefits that motivated its selection in the CRUTIAL modelling approach. However, this choice is not exclusive, and other formalisms presenting equivalent characteristics could also be used. It is noteworthy that additionally, a new formalism called “Dependent Automata” has been developed in the context of CRUTIAL to provide a rigorous definition of interdependencies related failures.

Significant contributions have been obtained by CRUTIAL considering the qualitative description of interdependencies related-failures and the quantitative assessment of their impacts on the dependability and security of electrical power systems services.

As regards the qualitative models, the main contributions include:

a) unified models considering accidental and malicious threats in a integrated way
b) a new formalism called Dependent Automata for describing interdependencies-related failures and its implementation into the DrawNet tool
c) a compositional modelling approach based on GSPNs to facilitate the generation of the qualitative models and to favour their reusability in other contexts
d) concrete examples for illustration based on selected scenarios.

Concerning the quantitative assessment models, template models have been developed capturing the structure, dynamics and failure propagation phenomena of the electrical power system entities, to be used to build complete models in generic control system scenarios. The formal definition of these models is based on the SAN formalism.

An ad-hoc simulator for EPS systems has been developed to support the definition and refinement of these template models by providing quick feedbacks on particular interdependencies related behaviour, although under some restricted system conditions.

III. TESTBEDS

III.1 Underlying assumptions

Distributed intelligence and secure interconnected communication networks constitute recognized key factors for the economic operation of electricity infrastructures in competitive power markets. Hence, electric power utilities need to extend risk management frameworks with adequate tools for assessing consequences of ICT threats on their critical business. This requires realistic probability estimates to cyber threat occurrences and consequent failure modes. Due to data sensitivity and rapid discovery of new vulnerability exploits, historical data series of ICT failures affecting power control infrastructures are not sufficient for a timely risk treatment. Such lack of data can partially be overcome by setting up testbeds to run controlled experiments and collect otherwise unavailable data related to cyber misbehaviours in power system operation.

Within the CRUTIAL project two testbed platforms have been set up for experimentally evaluating malicious threats on grid teleoperation and micro grid control scenarios.

The Telecontrol Testbed and the Microgrid Testbed have been chosen to investigate the transformation of the ICT infrastructure connecting power system components. There is a slow but steady to migrate from ad hoc communication infrastructures with dedicated protocols and dedicated hardware –often supported by a single SCADA vendor– towards a public standardised communication infrastructure that uses industrially standardised communication hardware and protocols. The communication hardware is not necessarily owned or controlled by the parties involved in the management of the grid, but often third parties provide the communication infrastructure which may be open to multiple users. Communication infrastructures and services may be offered by:

- telecom operators, renting their communication infrastructure to the power system operators;
- internet service providers, offering telecommunication services, which fulfil strict service-level-agreements with respect to guaranteed bandwidth and throughput, maximal latency, etc.;

while examples of shared usage of ICT infrastructures include:

- new parties resulting from the liberalisation of the electricity market, who share that communication infrastructure used by the classical system operators, but with restricted access to the information flowing through the network;
- new or emerging applications that locally exchange information to become larger entities, e.g. virtual power plants, or to provide new services, e.g. auxiliary services provided by dispersed energy resources. Another example concerns the usage of external information such as the instantaneous electricity price from real-time markets, which is incorporated into the control strategies in order to optimise economic benefits. Or intelligent loads can be switched on or off in order to implement demand response and avoid electricity peak costs, etc.;
- new control applications implementing manual and automatic defence actions in view of fully integrated wide area defence plans.

This leads to the fact that the communication infrastructure is less and less under the control of individual power system operators, and hence also that this infrastructure is less and less protected by the power system operators. Rather, the protection lies with such third parties

capability to fulfil the security, dependability and performance requirements of the changing and emerging control applications.
Furthermore, independence from a single SCADA-vendor drives for interoperability among different systems. In this context, there have been many standardisation initiatives in the previous decade, which are still ongoing. Such standardisation takes place at different levels (protocols, applications, among components, among systems, etc.).
If one extrapolates these trends further into the future, electric power systems nearly use internet-like technology for the different control operations (some of which have real-time constraints, others are less critical). Such commercial-off-the-shelf components, even in industrial grade, are by nature less dedicated than previous solutions.
From this perspective, the testbeds in the CRUTIAL project make use of TCP/IP as a communication protocol on top of dedicated internet-like connections, possibly extended by protection mechanisms such as Virtual Private Networks (VPN) or other security-enhancing techniques. It is clear that industrial practice has not yet finished such evolution, and that the power industry is not using (and will not be using) plain internet technology without conservative precautions.

In the CRUTIAL testbeds the focus has been on the impact of ICT faults on power control algorithms. It is obvious that when the electrical grid goes down and no precautions have been taken (such as uninterruptible power supply) it might be that the ICT system itself goes down as well as a result of this, hampering recovery. These scenarios have not been considered in the testbeds, as we assumed that sufficient precautions were taken to ensure independence.

III.2 Exploitable knowledges

The CRUTIAL testbeds [4] are composed of two platforms. One platform – the Telecontrol Testbed – consists of power station controllers on a real-time control network, interconnected to corporate and control centre networks. The other platform – the Microgrid Testbed – is based on power electronic converters that are controlled from PCs that are interconnected over an open communication network.
Both testbeds integrate elements from the Electrical Infrastructure as well as from the Information (computing and communication) Infrastructure, in order to focus on their interdependencies, and specifically on the vulnerabilities that occur in the electric power system when a part of the information infrastructure breaks down. These testbeds have been used to investigate

- local, hierarchical and distributed control scenarios at transmission and distribution level;
- how architectural patterns for enhancing robustness can be integrated in a realistic setup;
- which interdependencies occur in practice.

The two testbeds are complementary. The Telecontrol Testbed focuses on the operation and supervision of a distribution grid (high and medium voltage levels) with classic (local and hierarchically distributed) control algorithms. The Microgrid Testbed focuses on a distribution grid (low voltage levels) with innovative (local and decentralised, distributed) control algorithms. Results from experimental campaigns on the two testbeds have been analysed by means of an evaluation framework.

The Telecontrol Testbed implements load reduction scenarios which may occur in power conditions presenting different degrees of severity. Load reduction usually occurs when the power system is exposed to disturbances due to deficiency conditions (faults, loss of generation, switching errors, lightning strikes, etc). Major disturbances may have a dramatic impact on the performance of the power system, requiring fast and reliable load shedding

actions which must be set and timed properly: inappropriate load reduction caused by the execution of an improper load shedding scheme may be inefficient and even cause cascading effects.
The testbed applications have been stressed by a sequence of DoS attacks to demonstrate the increasing severity of their effect on the implemented control functions: first the denial of the supervision function and control activities, then the preclusion of the manual intervention of the grid operator, and last the denial of the execution of automatic actions in full emergency conditions. The evaluation of results from attack experiments presented in [4] showed that flooding based DoS attacks have severe effects on IEC 60870-5-104 communications in terms of both loss of messages and total block. The identified experimental measures constitute a contribution to Part 7 of the standard IEC 62351 for the security through network and system management, currently under development with the Technical Committee 57 of the International Electro technical Committee.

The Microgrid Testbed has been running primary and secondary microgrid control algorithms on power electronic inverters equipped with IED, connected both electrically (via a power network) and logically (via a communication network). These control algorithms interact via the power network to control voltage and frequency (primary control). They interchange messages via the communication network allowing secondary control to maintain voltage levels. The impact of fail-silent ICT faults is comparable to changing the periodicity of message exchange and hence to slower adaptation of the invertors to generator/consumption changes. The impact of arbitrary failures may lead to over- or undervoltages, which will trigger the electrical protection and calls for other fault prevention or tolerance solutions.

IV. ARCHITECTURE, SERVICES AND PROTOCOLS

The largely computerized nature of critical infrastructures on the one hand, and the pervasive interconnection of systems all over the world, on the other hand, have generated one of the most fascinating current problems of computer science and control engineering: how to achieve resilience of critical information infrastructures. The project CRUTIAL was concerned with the susceptibility of the latter to computer-borne attacks and faults, i.e., with the protection of these infrastructures. An architecture and a set of techniques and algorithms have been proposed aiming at achieving resilience to faults and attacks in an automatic way.

Although inspired by previous intrusion-tolerant system architectures, the CRUTIAL architecture was largely influenced by two facts.

Firstly, the fact that Critical Information Infrastructures (CII) feature a lot of legacy subsystems such as controllers, sensors, actuators, etc.

Secondly, the fact that conventional security and protection techniques can bring serious problems, when directly applied to CII controlling devices, by preventing their effective operation. Although they are very practical problems, they yielded in fact very interesting research challenges.

Another relevant fact was the consortium's belief that the crucial problems are mostly created by the generic and non-structured network interconnection of CIIs, which bring several facets of exposure impossible to address at individual level. Whilst it seems today non-controversial that such a status quo brings a considerable level of threat, to the consortium's knowledge there had been no previous attempt at addressing the problem through the definition of a reference model of a critical information infrastructure distributed systems architecture. The project intended a model which, by construction, would lay the basic foundations for the necessary global resilience against abnormal situations. The consortium's conjecture was that such a model would be highly constructive, for it would form a structured framework for

1. conceiving the right balance between prevention and removal of vulnerabilities and attacks;
2. achieving tolerance of remaining potential intrusions and designed-in faults; and
3. enabling adaptation and self-awareness mechanisms to overcome unforeseen situations.

Finally, and in a related manner, the consortium conjectured that any solution, to be effective, has to involve automatic control of macroscopic command and information flows, occurring essentially between the several realms composing the critical information infrastructure architecture (both intra- and inter-organizations), with the purpose of securing appropriate system-level properties, at organizational level. This has to be addressed, in an automatic way, through innovative access control models that understand the organizational reality, and are thus capable of translating the related high-level security policies into the adequate technical mechanisms such as access control matrices and firewall filter rule-sets.

The CRUTIAL Architecture [5] intends to reply to a grand challenge of computer science and control engineering: how to achieve resilience of CII, in particular in the electrical sector. It consists of main architectural options and components, with a special emphasis on a protection device called the CRUTIAL Information Switch (CIS). Given the various criticality levels of the equipments that have to be protected, and the cost of using a replicated device, the project defined a hierarchy of CIS designs incrementally more resilient. The different CIS designs offer various trade offs in terms of capabilities to prevent and tolerate intrusions, both in the device itself and in the information infrastructure. The Middleware Services, APIs and Protocols together represent the CRUTIAL approach to intrusion tolerance.

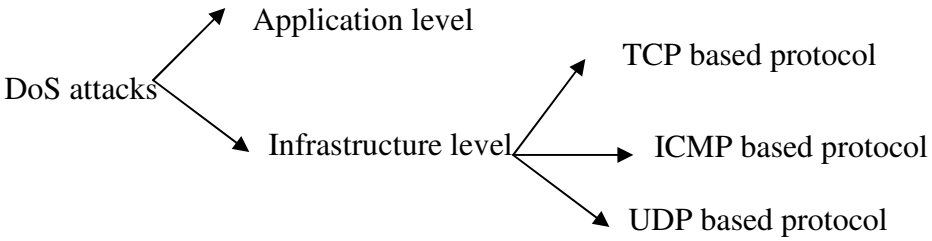
The CRUTIAL middleware comprises several building blocks that are organized on a set of layers, each one providing services to other layers or directly to the applications.

- √ The Multipoint Network layer is the lowest layer of the middleware, and features an abstraction of basic communication services, such as provided by standard protocols, like IP, IPsec, UDP, TCP and SSL/TLS.
- √ The Communication Support layer features three important building blocks: the Randomized Intrusion-Tolerant Services (RITAS), the CIS Communication service and the Fosel service for mitigating DoS attacks. The RITAS are organized as a stack of randomized intrusion-tolerant protocols, supporting applications who depend on intrusion-tolerant broadcast and agreement. These protocols, being randomized, overcome the impossibility result in asynchronous settings (also called the FLP result), but present a significant performance improvement over previous protocols of the same class. The CIS Communication service supports secure communication between CIS and, ultimately, between LANs (Local Area Networks). It provides secure channels, multicast primitives, and probabilistic gossip-based information diffusion between CIS. The Fosel filter addresses the DoS problem with an overlay protection layer for DoS attacks on top of the normal infrastructure.
- √ The Activity Support layer comprises the CIS Protection service and the Access Control and Authorization service. The CIS Protection service protects realms from one another, i.e., a LAN from another LAN or from the WAN, thus allowing to deal both with outsider and insider threats. The Access Control and Authorization service is implemented through PolyOrBAC, which defines the rules for information exchange and collaboration between sub-modules of the architecture, corresponding in fact to different facilities of the CII's organizations. Each organization specifies its security policy according to OrBAC. As organizations are interconnected through CIS, each CIS regroups mechanisms to define security policy of systems that compose each LAN (local and collaboration policies), and it also includes mechanisms based on web-services for collaboration: to make these LANs capable of collaboration and offering services to each other. The interactions between the organizations are defined by "e-contracts", and are checked at run-time against a timed-automaton model of the contracts. Such a model-checker aims to detect any abuse by an organization of pre-established e-contracts, and to gather evidence to convince a judge about the abuse.
- √ The Monitoring and Failure Detection layer is devoted to monitoring and failure detection activities. Diagnosis in CRUTIAL should occur at different components at different architectural levels, and as such, the classical framework has been extended: several components need to be monitored and several deviation detection mechanisms need to be in place, errors observed in different components must be correlated. Likewise, given that the project is dealing with a complex infrastructure, methods for distributed diagnosis are mandatory, with a distinction between local and global detection and diagnosis.
- √ The Runtime Support chapter features as a main component, the Proactive-Reactive Recovery Service, whose aim is to guarantee perpetual execution of any components it protects. CRUTIAL investigated limitations of existing approaches to intrusion-tolerant proactive recovery, and proposed a very complete scheme addressing them, named proactive-reactive recovery within the project. The consortium's first observation is that protecting oneself from timing attacks by using asynchronous models, and fulfilling periodic recoveries, are incompatible goals. To address this issue, the project proposed an innovative scheme based on a hybrid sync-asynchronous architecture, called proactive resilience. The consortium's second observation is that one should allow correct replicas that detect or suspect that some replica is faulty, to accelerate the recovery of this replica. It is known that perfect Byzantine failure detection is impossible to attain in a general way. In

consequence, dealing with imperfect failure detection is the most complex aspect of the proactive-reactive recovery service developed.

IV.1 Coverage of attack models

The Fosel architecture on its own is only resistant to DoS attacks and it does not cover intrusion attacks. Intrusion detection and protection is however supported by the CIS protection services [5]. With specific reference to DoS attacks, the following high level DoS attack classification is introduced to clarify their coverage in the CRUTIAL architecture.



- Application level DoS attacks (covered by the CIS protection service): attackers attack through the application interface; for example, attackers overload an application by sending abusive workload, malicious requests which lead to application crash, extra CPU processing, system reboot, or general system slowing down. In this type, an attacker can also render a computing resource unavailable by modifying the system configuration (such as its static routing tables or password files). In fact attackers attack the system by exploiting **weaknesses in the application software**. This type of vulnerability typically originates in ***inadequate software assurance testing or negligent patching***. Such DoS attacks are generally addressed through *hardened security policies and authentication mechanisms* ***(in the CRUTIAL project this type of attack is covered by the CIS protection service)***.

- Infrastructure level DoS attacks (covered by the Fosel architecture): attackers directly attack the resource of the service infrastructure, such as the networks and hosts of the application service; for example, attackers send flood of bogus packets to saturate the target network. Only IP of victim is enough for attack and no more information is required. This model of attack is known as a DoS attack and can be classified based on communication protocol: TCP based, ICMP based and UDP based. ***This attack model is covered by the Fosel architecture***. *Fosel handles all Infrastructure DoS attack types.*

  Although in the Fosel evaluation performed in CRUTIAL only UDP based protocols have been evaluated, Fosel handles other DoS attacks (TCP; ICMP) as well. Because Fosel architecture is independent of attack pattern and protocol models. Fosel does not verify signature. It does not decrypt payload. It does not verify protocol. It just sees the IP source of the packet. If the IP source is IP of the Green node, packet is accepted, otherwise it is dropped. Hence ***Fosel is independent of protocols, signatures and attack patterns and can support all types of DoS attacks.***

  About the resistance of the overlay networks against attacks, it has to be noted that the location of green nodes is chosen randomly and their location is hidden for the attackers. If one green node is accidentally attacked, the target node randomly selects another overlay node as a green node.

For a second note, the overlay network (as Chord has been used within CRUTIAL with Fosel) has a dynamic nature and uses random path diversity (RPD technique) to handle DoS attack on the overlay. In fact the dynamic nature of overlay within RPD technique is strong enough to handle attacks such as DoS on the overlay and also routing path discovery [7].

The CRUTIAL consortium is extremely proud that parts of the CRUTIAL architecture and protocols allowed to Paulo Sousa, a LaSIGE PhD researcher from the CRUTIAL team, to win 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.

V. ANALYSES AND EVALUATIONS

The assessment activities performed in CRUTIAL addressed three central elements:

1. the attacks to the ICT infrastructure
2. the architectural solutions devised by the project, and
3. the (inter)dependencies between the Electrical Infrastructure (EI) and the Information Infrastructure (II).

For what concerns attacks, the consortium developed a tool (AJECT) that allows to emulate various type of attacks, and that has been used to collect experimental data of the CIS behaviour under attack.

To get a more realistic view of ICT attacks, the consortium worked on the data collected from a set of honeypots. Honeypots have been modified to allow to collect data also on specific attacks to SCADA systems and to capture more complex attack behaviour through the use of high-level interaction honeypot. The data collected from these honeypots provided useful insights about malicious activities considering different perspectives (depending on the level of interaction offered to the attackers and the services exposed by the honeypots). These data have been statistically elaborated to estimate the distribution of inter-attack time, thus giving a more precise indication of the statistical nature of attacks, and allowing the use of honeypot-collected information also in the model based evaluation [7].

The architectural solutions have been studied through models and through experimental work with the available prototypes. The work concentrated on the two main pillars of the CRUTIAL architecture, namely FOSEL (Filtering with the help of Overlay Security Layer) and CIS (Crutial Information Switch), both the CIS-CS (Communication Service) and the CIS-PS (Protection Service).
The objective of the analysis performed has been the evaluation of the effectiveness of the proposed components from the point of view of the dependability improvements they bring, as well as the performance overhead introduced by their implementation.

In particular the FOSEL experimental analysis aimed at deriving a good characterization of the parameters of the protocol (number of replicas, percentage of messages dropped without analysis) in situations of attacks to an application site and to the overlay network deployed by FOSEL.

CIS-PS has been analysed through models and with a large sets of experiments on the CIS prototypes. Models have been devised for both the basic CIS-PS-IT (Intrusion Tolerant), to study its correctness, and for the more complex CIS-PS-SH (Self Healing), were models have been used to study and compare the various strategies of self-healing. A large set of experiments has been conducted on a prototype implementation of CIS to assess its efficacy in a real context characterized by various forms of attacks. The communication service of CIS has instead been studied using a large set of simulation experiments.

For what concern interdependencies, CRUTIAL brings a very innovative contribution to the current literature on system evaluation: indeed the problem has been scarcely studied in the past, also due to the complexity of having to take into account two very different types of systems: the EI, whose state is a complex mix of continuous and discrete variables and the II, that typically has a discrete state, but whose behaviour may change over time (e.g. the non-homogeneous behaviour of DoS). The solution devised in the CRUTIAL Modelling Framework has been put into work on the control system scenarios also developed in the Telecontrol Testbed. In particular the SAN models (that constitute the very detailed model in the Framework) have been exercised under a number of parameters for a couple of reference IEEE electrical grids, in a situation in which DoS makes a subset of the power

substations unreachable. The study mainly addressed the ability of the system to recover from an electrical failure, while a DoS attack is making defence actions not applicable.
The Modelling Framework has been enriched by devising an interaction between the very detailed model based on SAN, that is able to consider the structure of the power grid, its behaviour, and an abstract representation of the control, and the intermediate model based on SWN that allows a detailed description of the control system scenarios.

VI. AN INTEGRATED VIEW OF CRUTIAL RESULTS

A high number of dependencies exist among the CRUTIAL results which required intensive interactions among partners' activities during the project running. The Figure 1 illustrates a simple roadmap showing the way in which the different strands of the work across the project were integrated.

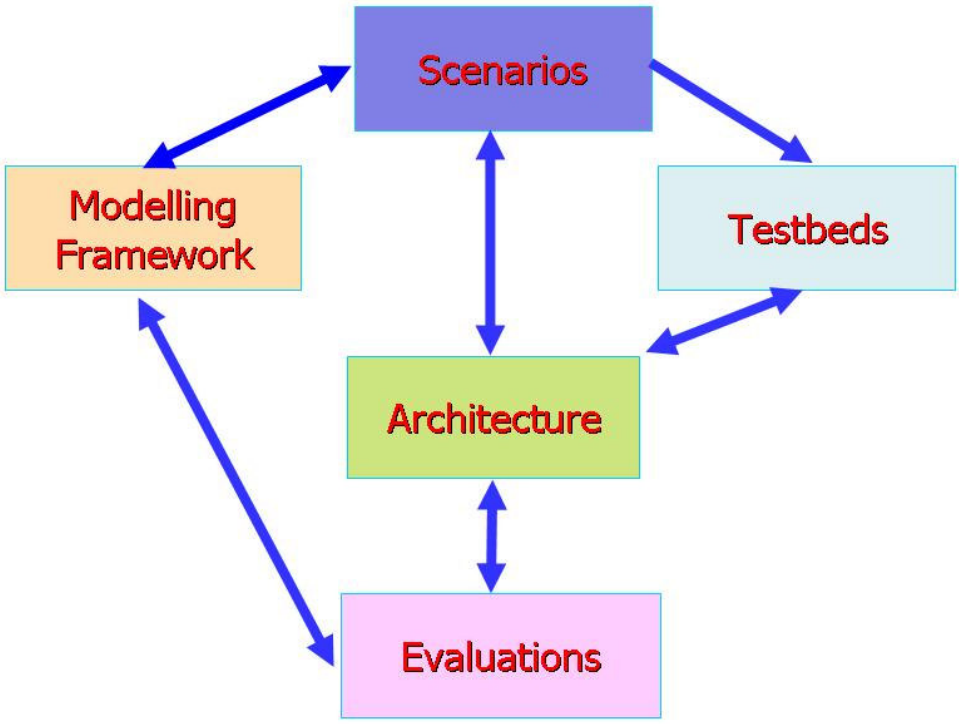


Figure 1: CRUTIAL Roadmap.

Following the arrows in the roadmap above, the main relationships among the CRUTIAL results may be identified, for instance

1. Scenarios were used for ì) the application of the Modelling and Evaluation Framework; ii) the Testbeds development; iii) the development and demonstration of the Architectural Components;
2. Architectural Components were i) used in the model based and experimental validation activities; ii) integrated into the Microgrid Testbed.

The concerted work performed by the CRUTIAL consortium allowed to produce a set of partially integrated results. A more advanced level of integration may be achieved by future collaborative activities (see also the CRUTIAL exploitation plans in [8]).
The following sections identify the possibilities of integration among the CRUTIAL results.

VI.1 Modelling Framework

The Figure 2 shows an integrated view of the qualitative and quantitative components of the Modelling Framework.

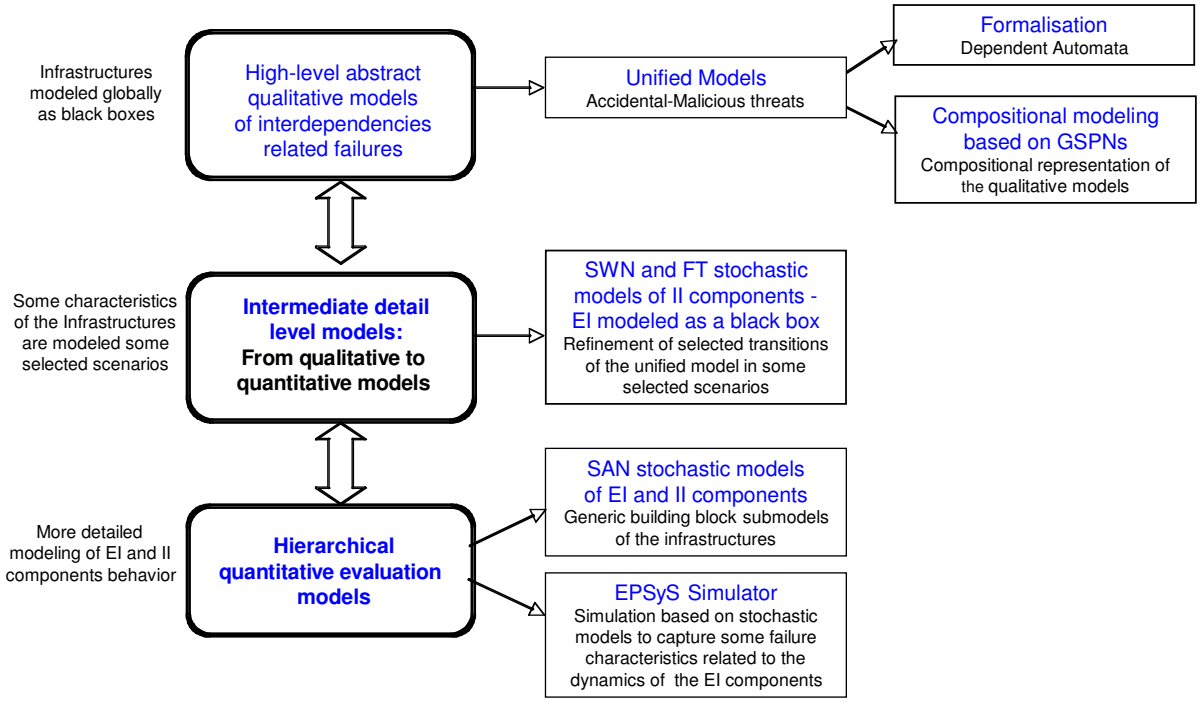


Figure 2: Components of the Modelling Framework.

VI.2 Fosel and CIS

With reference to the integration of the architectural components, the Fosel selective filter may be considered a service offered by the CIS. The overlay network of the Fosel architecture resides in the WAN. In other words the CIS communicate through the overlay on the top of the WAN. The Figure 3 shows the functional link between the Fosel architecture and CIS.

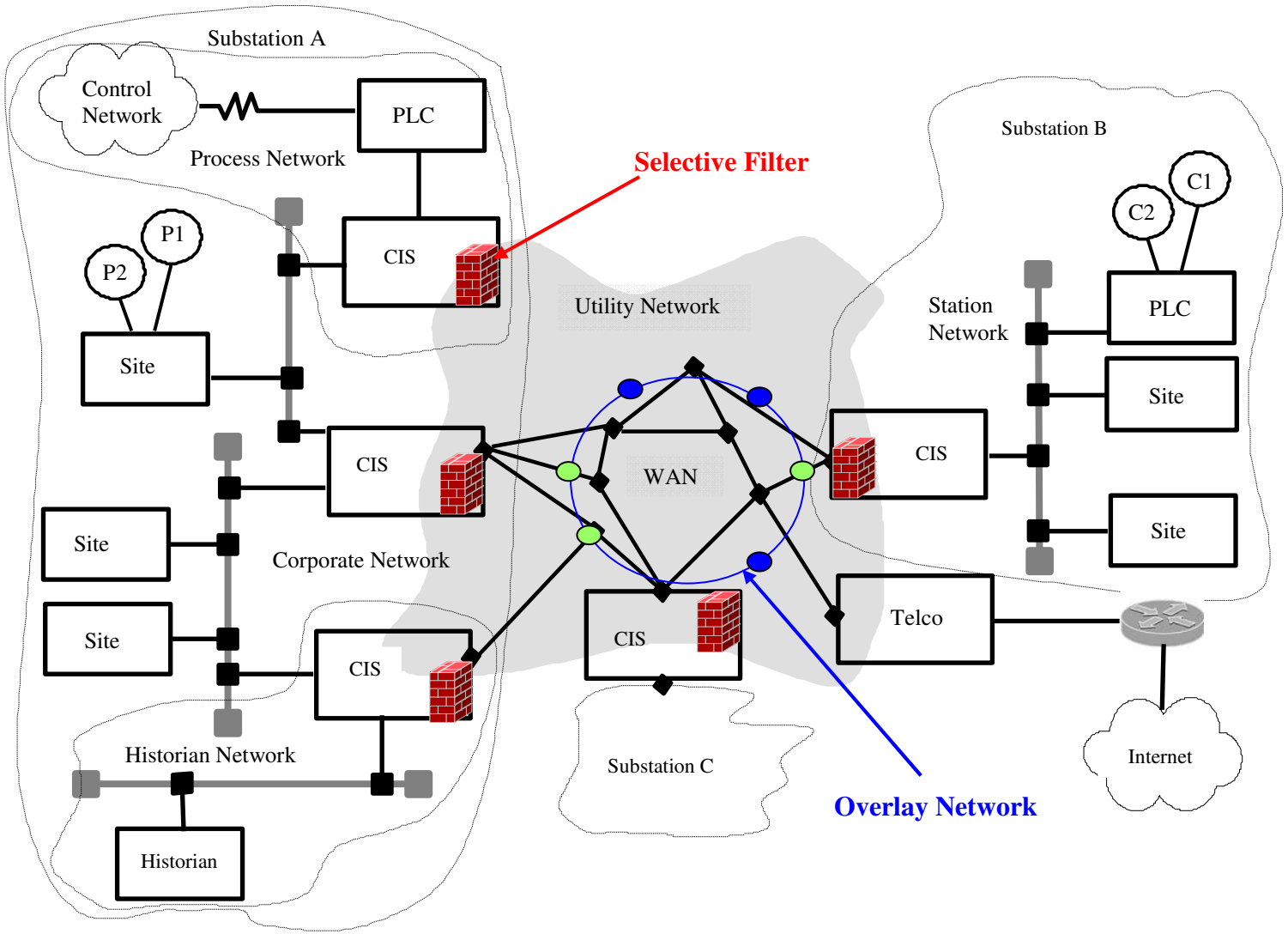


Figure 3: Fosel and CIS.

VI.3 PolyOrBAC and CIS

The PolyOrBAC access control framework has been designed to be implemented in the CISs. The CIS should include the mechanisms for enforcing the local security policy of the organization protected by the CIS and for managing external accesses and interactions between organizations protected by different CISs, through the use of e-contracts and timed automata. From a practical point of view, the implementation of the PolyOrBAC framework inside the CIS will require the interception of the messages and communications going through the API of the CIS in order to be able to check at run-time the validity of the accesses according to the local timed automata. Such implementation should be feasible without a great difficulty and we do not foresee at this stage technological problems against it. The adoption of the web service technology for managing the interactions between different CISs should also facilitate the implementation and the deployment.

VI.4 Testbeds

The Telecontrol Testbed, developed in CRUTIAL as separate platforms for evaluating resilience to attacks in complementary control schemes, could be further developed in an integrated testbed supporting the evaluation of mixed centralised/distributed control schemes. Many distributed microgrid applications, such as those experienced on the Microgrid Testbed, will provide monitoring data to centralized control centres within the perimeter of the distribution system operator (DSO) or of an area control centre (ACC). This monitoring data can be complemented by control signals from the DSO or ACC to shed loads or curtail generation. Such centralized systems imply teleoperation and are hence vulnerable to the attacks as evaluated in the Telecontrol Testbed.

VI.5 Testbeds and Architecture

The Microgrid Testbed architecture integrates the Fosel filter. The whole WAN of LANs model, where CIS extended with Fosel and PolyOrBAC provide resilient connectivity and access control among control sides, perfectly fits with the architecture of both Testbeds. The following figure instantiates the Architectural Components with the Telecontrol Testbed platform.

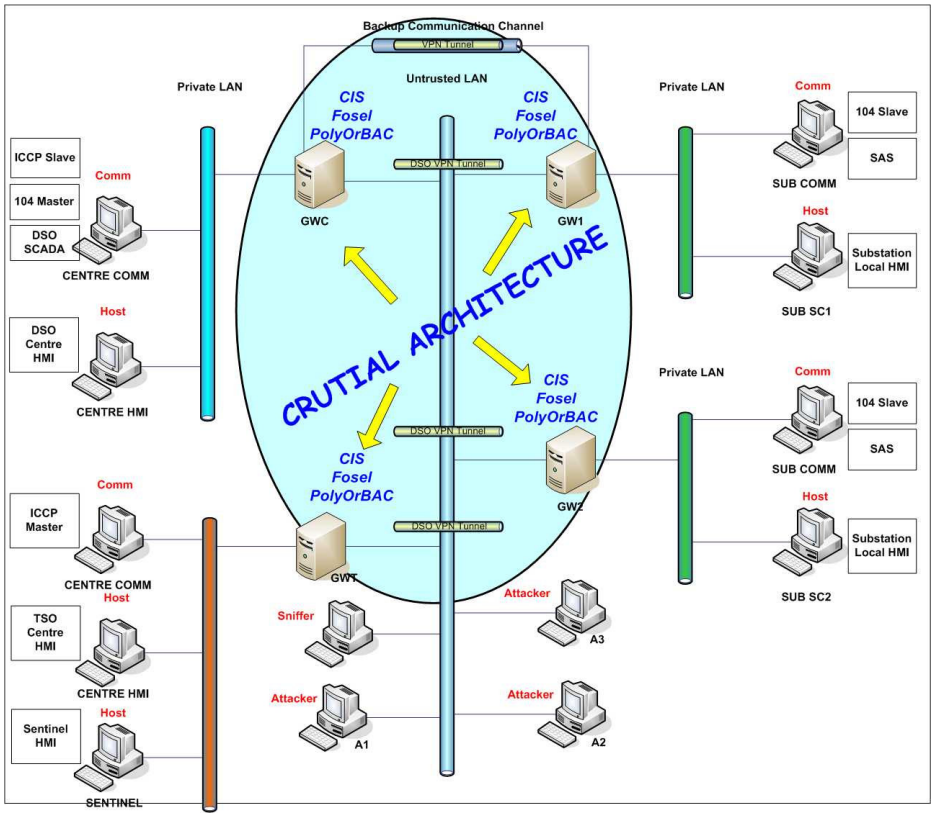


Figure 4: CRUTIAL Architecture in the Telecontrol Testbed.

VI.6 Testbeds and Model Based Evaluation

In the course of CRUTIAL, the same scenarios developed in the Telecontrol Testbed have been used as test cases for the application of the model based evaluation techniques supported by the quantitative components of the Modeling Framework. A stronger integration between the testbed measurements and the model based evaluation may be addressed in a future research activity.

VI.7 Testbeds and Experimental validation

The testbed experimental activity may be expended by attack data collection through the SCADA honeypot architecture developed in CRUTIAL, and attack injection techniques supported by the CRUTIAL AJECT tool.

VII. DISSEMINATION

From the very beginning of the project lifetime the CRUTIAL consortium identified several major means and actions as effective and powerful to disseminate the project's achievements. Such actions had to assure their prompt and wide spreading. A detailed description of the dissemination actions undertaken during the project lifetime has been reported in [8], 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 mean 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 [8];
- 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.

Table 1 provides an overview of the means adopted for the dissemination of CRUTIAL knowledge.

Actual date	**Type**	**Type of audience**[1]	**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
15 March 2007 - 3 February 2009	Thematic workshops	Research, academic, industrials, standardization bodies, public authorities, …	Mainly EU	CESI-R + ALL

Table 1: Overview of the dissemination means.

The project web site, maintained by CESI-R, constituted an important mean 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 mean of assessing the level of interest arisen by the CRUTIAL project, a statistical analysis on the project web accesses during the first three years has been performed. The obtained numbers are more than positive, as can be derived from the Figure 5 referred to the accesses in the third project phase.

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

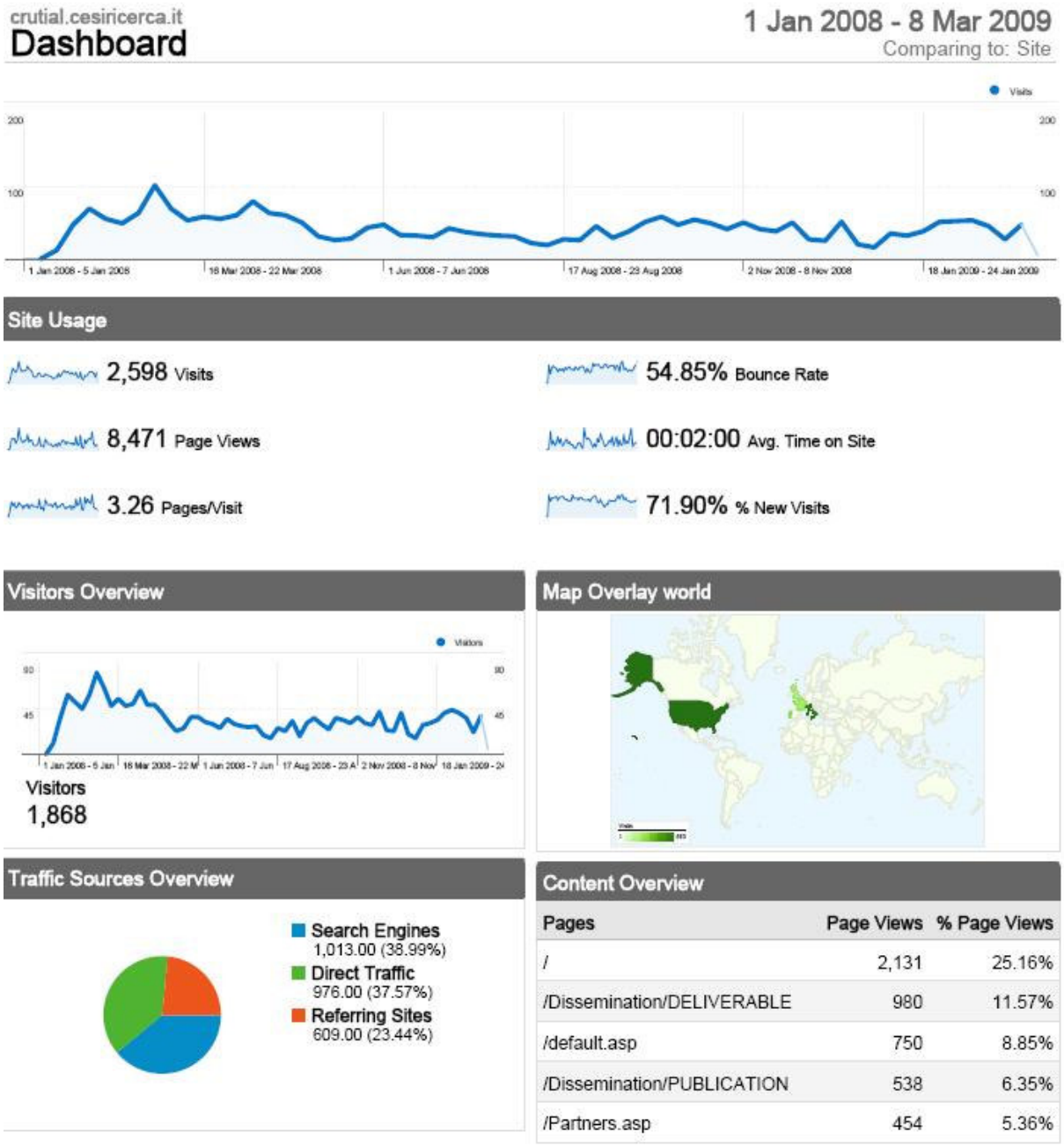


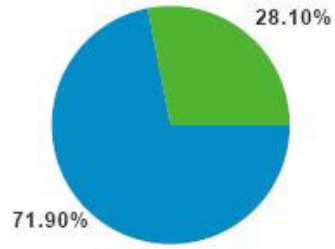
Figure 5: Statistics – summary.

Comparing these results with those obtained at the end of the second year, the number of accesses to the web site has being kept high, with more than 28% of returning visitors (Figure 6), an increasing interest from a high number of geographically distributed cities (Figure 7) from worldwide countries (Figure 8). The high interest for CRUTIAL from the United States is still confirmed, followed by Italy.

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

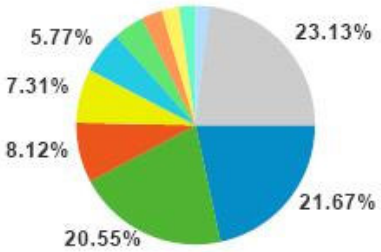
Figure 6: Traffic Sources Overview.

2,598 visits came from 806 cities

Figure 7: 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%

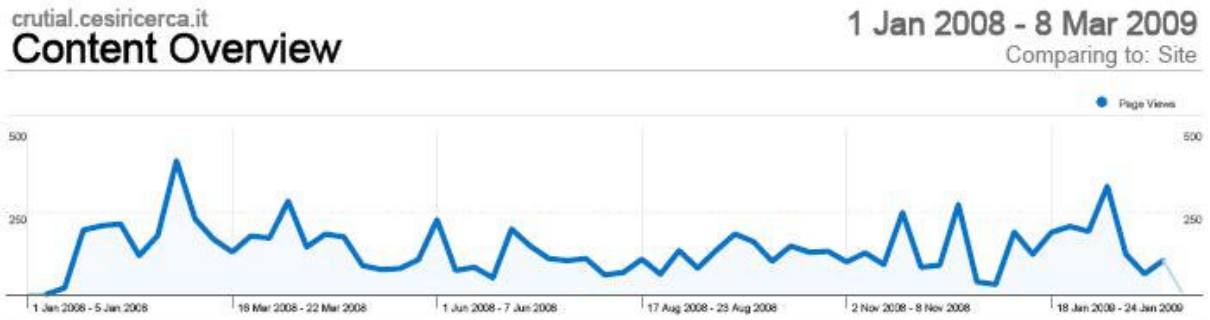
Visits



1 - 10 of 82

Figure 8: Percentage distribution of visiting countries.

Also from the point of view of documents downloads, the numbers increased a lot during the last year, and interested the deliverables and publications documenting the major achievements of CRUTIAL (Figure 9).



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 9: Content Overview.

A consistent amount of publications reporting CRUTIAL activities and results has been produced during the project lifetime, including journal articles, book chapters and papers in conference proceedings. In addition, it is also worth to mention a number of publications related to CRUTIAL activities but without explicit acknowledgement to the project. Presentations related to CRUTIAL themes at relevant events (such working group meetings and European project workshops) constituted another important aspect of dissemination of project's achievements. Figure 10 and Figure 11 show summaries about these forms of dissemination.

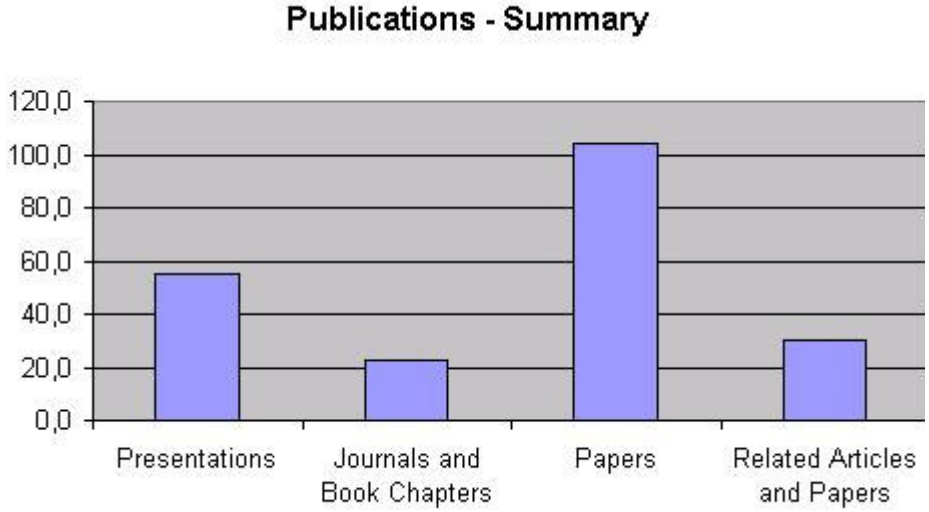


Figure 10: Summary of CRUTIAL Publications.

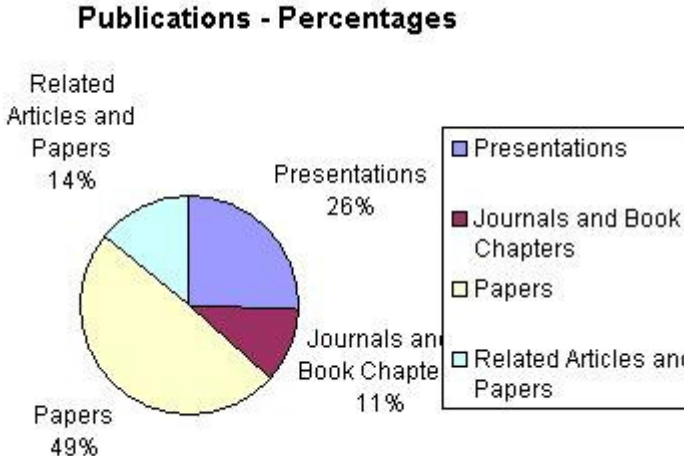


Figure 11: Relative percentages of CRUTIAL Publications.

The project partners established 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 work programme, both at European and American

levels. The CRUTIAL consortium was aware of a number of related programmes/projects/initiatives and established contacts with those listed in the Table 2 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).

Title	Type	Start date- End date	Website
Cigré WG D2.22– Treatment of Information Security for Electric Power Utilities	International Working Group	30/08/2006 30/08/2010	http://www.cigre.org/
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	2000-2008	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/
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 2: EU projects liaised with CRUTIAL.

VII.1 Feedback from industrial stakeholders

Since the very beginning of the project the consortium recognised that a way to increase the chance of developing something that has broad acceptance among the utilities is to deepen the relation and collaboration with working groups participated by industries from the power sector. By the membership of the Project Manager to the Cigré Working Groups related to CRUTIAL topics, the consortium had the possibility of receiving inputs by daily information security users from power utilities in several countries. Some of those members were also directly involved in the Industrial Advisory Board (IAB) of the CRUTIAL project.

The CRUTIAL IAB was populated by organisations operating in the power generation, transmission and distribution sectors, and by system vendors. The geographic distribution of its members overcome the national borders of the CRUTIAL participants, covering a wide European territory, from north to south (Norway, Portugal, Italy, Sweden, Scotland, Germany). Power System Authorities and Regulators were not represented in the project Board and this was considered a missing voice in the pool of interested stakeholders.

Along the project running, the IAB members have been involved in the validation of the CRUTIAL preliminary achievements, including the control system scenarios. The project deliverables were sent before of making them publicly available and corresponding presentations were made during face to face meetings. The feedback from the IAB was related to both the whole CRUTIAL project and to specific CRUTIAL advancements.

Several technical meeting between CESI RICERCA and ENEL took place during the course of the project, aimed at showing the progress done on the Telecontrol Testbed in the CESI RICERCA laboratory and sharing information about the status of the ICT infrastructures supporting operation and maintenance activities of a Distribution System Operator. 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. ENEL expressed full satisfaction on the work done and encouraged to continue the resilience assessment of telecontrol infrastructures.

The project registered a high attendance and active participation during the CRUTIAL workshops, both IAB workshops organised by CRUTIAL and joint Workshops with GRID and IRRIIS projects organised by the Commission, including

- √ a presentation from the convener of the Cigré JWG D2/B3/C2.01 to the IAB workshop in Leuven
- √ an invited speech by ENEL at the joint Workshop in Brussels
- √ a presentation by Statnett at the IAB workshop in Milan
- √ active participation by Siemens in the Round Tables of both joint Workshops in Brussels.

From the IAB feedback the consortium had the confirmation that the information exchange/flow was very good and it could not be better. Some difficulties were expressed in relation to the time required to read the project documents. Notwithstanding all contributions have been evaluated of a very good quality and very fruitfully: the CRUTIAL objectives were addressing the right topics, the project approach was judged very systematic. The level of presentations at CRUTIAL meetings was judged good enough, also considering the recognised difficulty in finding an appropriate level that suites the heterogeneous members' competences.

One point that has been stressed was that from the utility perspective, it was important that the work and the outcome of CRUTIAL was practical, concrete and "easy-to-use". IAB members also involved in Cigré encouraged the exchange of experience with the Cigré WG D2.22 on Treatment of Information Security for Electric Power Utilities. To have IAB meetings was considered very good but for a day meeting the amount of travelling expenses and required time was considered very high. The consortium was invited to consider a chance to combine such meetings with other workshops or conferences which were in line with similar topics.

Following IAB suggestions i) the next IAB workshop in Milan (CESI-R) was planned just before the Cigré D2.22 meeting in Florence (hosted by TERNA); ii) industrial stakeholders have been approached one by one; iii) slides have been used for high-level briefings to encourage interest; iv) feedback has been reverted back to the project.

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).

The second event related to dissemination activities towards industry was the workshop devoted to IAB members, which took place at CESI RICERCA premises on 6 March 2008. Challenges and R&D needs related to ICT security were presented by a Transmission System operator's representative. 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.

Several of the presented needs constitute the core motivations of the CRUTIAL project. The CRUTIAL achievements were illustrated by the consortium. The comments by the present IAB members were positive and encouraging on the continuation along the same track.

The final CRUTIAL 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.
The workshop started with an introduction by Dr. Jacques Bus, Head of the Unit INFSO F5 «Trust and Security», who presented the latest EU developments on CIP (Critical Information Protection). 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 technical 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.
A round table, chaired by Dr. Jacques Bus and participated by six industrial panellists invited by the two projects, concluded the workshop. 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 on 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.

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.

Siemens confirmed that the consideration (modeling and test bed) of impact of ICT components on power grid has high relevance for their business units and in particularly for their research & technology department. Siemens was very positively impressed by the CRUTIAL presentations at the final Workshop and invited the project coordinator to find out occasions for a fruitful exchange of experience and mutual information on the research developed by CRUTIAL.

The CRUTIAL dissemination towards the Cigré WG D2.22 allowed a fruitful discussion and cross-references in published papers: for instance CRUTIAL documents about interdependencies modelling have been referenced in Cigré papers related to cyber risk assessment of power control systems. This represents an optimal vehicle for the dissemination of the CRUTIAL exploitable knowledges in the world wide power system community participating to the Cigré organisation.

VIII. EXPLOITATION

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. 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.

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.

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.

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 (incl. 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 an 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.

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.

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.

In CRUTIAL the interdependencies analysis 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.

From the point of view of the CRUTIAL architectural solutions and protection mechanisms, the developed designs can be deployed by industrial partners to protect their critical information infrastructures. Although the project focused on the computer systems behind electrical utility infrastructures, 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.

Considering the CRUTIAL Access Control model and mechanisms, the proposed PolyOrBAC framework offers each involved organization the capacity of collaborating with the other ones, while maintaining a control on its resources and on its internal security policy. This is an important characteristic that should allow the use of PolyOrBAC in other infrastructures than those investigated in CRUTIAL. Also the use of the web services technology to implement the interactions between organizations is another noteworthy attractive advantage that should facilitate the adoption of PolyOrBAC by other communities and the development of commercial tools implementing the proposed framework.

The CRUTIAL Testbeds represent embrionic control infrastructures for assessing the resilience of grid control systems to cyber threats that may evolve in several future directions.

The Telecontrol Testbed provides a scaled-down 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. Its Evaluation Framework consists of repeatable experiments and metrics used in the project for deriving experimental results on the effectiveness of Denial of Service experiments on secure IEC 60870-5-104 communications. Such results will be made available to the interested communities (industrial, technical and scientific).
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).

In the last phase of the project, the Telecontrol Testbed exploitation capabilities arose the interest of both industries and ongoing European initiatives in the frame of the establishment of the European Reference Network for Critical Infrastructure Protection (ERN-CIP).

The Microgrid Testbed is also a platform for other researchers that elaborate different electrical or control aspects of distributed energy sources. Among other projects, the testbed will pay a pivotal role in a next (regional) project on smart grids.

Both CRUTIAL Testbeds has been evaluated by the ESTEC project conducting a feasibility study on an European Network of SCADA Test Security Centres for Critical Energy Infrastructures.

Detailed information about the exploitation of the CRUTIAL results may be found in [8].

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 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.

Specific efforts need to be devoted by the involved communities (the Electric Power community and the Information Technology community) to influence the technological progress in order 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 introduction of a competitive electric power market.

Having the CRUTIAL developments addressed these needs, the results obtained by the project are aimed at providing insights to Electric Power companies and standardization bodies for exploiting resilience in critical utilities infrastructures. Consequently they will contribute to reduce the power system disservices clearly having a large social and economic impact.

The CRUTIAL results will help in designing and assessing new Electric Power systems and information infrastructures and will constitute an important asset in the European technical arena, to be used by electrical utilities R&D, planning, technology and engineering departments, to stimulate what the CRUTIAL consortium foresee as a dramatic improvement in the overall quality and resilience of electrical utilities infrastructures. The consortium's foresight is that the take-up of these solutions will happen in coordination of the above-mentioned departments, with the several suppliers and providers involved: SCADA

suppliers; information systems integrators; intranet/extranet/Internet service and infrastructure providers.

If the envisioned follow up will happen, in the next five years following the project end the benefits of the CRUTIAL results will be able to reach all European citizens, who will continue experiencing an high reliability level of the electricity supply despite of the many technological evolutions and the liberalisation of the electrical market.

REFERENCES

[1] F. Garrone, C. Brasca, D. Cerotti, D. Codetta Raiteri, A. Daidone, G. Deconinck, S. Donatelli, G. Dondossola, F. Grandoni, M. Kaâniche, T. Rigole, “Analysis of new control applications”, CRUTIAL Project, Work Package 1 - Deliverable D2, http://crutial.cesiricerca.it, January 2007

[2] M. Kaâniche, S. Bernardi, A. Bobbio, C. Brasca, S. Chiaradonna, D. Codetta Raiteri, F. Di Giandomenico, G. Dondossola, G. Franceschinis, F. Garrone, A. Horvath, K. Kanoun, J.C. Laprie, P. Lollini, J. Sproston, “Methodologies synthesis”, CRUTIAL Project, Work Package 2 - Deliverable D3, http://crutial.cesiricerca.it, January 2007

[3] M. Kaâniche, M. Beccuti, A. Bobbio, C. Brasca, S. Chiaradonna, S. Donatelli, F. Di Giandomenico, G. Franceschinis, K. Kanoun, J.-C. Laprie, P. Lollini, F. Romani “Final version of the modelling framework”, CRUTIAL Project, Work Package 2 - Deliverable D16, http://crutial.cesiricerca.it, March 2009

[4] G. Deconinck, H. Beitollahi, T. Loix, G. Dondossola, F. Garrone, J. Szanto, “On EPS-ICT interdependencies in the testbed”, CRUTIAL Project, Work Package 2 - Deliverable D17, http://crutial.cesiricerca.it, March 2009

[5] A. Abou El Kalam, A. Baina, H. Beitollahi, A. Bessani, A. Bondavalli, M. Correia, A. Daidone, W.r Dantas, G. Deconinck, Y. Deswarte, F. Grandoni, H. Moniz, N. Neves, P. Sousa, P. Verissimo, “Architecture, Services and Protocols for CRUTIAL”, CRUTIAL Project, Work Package 4 - Deliverable D18, http://crutial.cesiricerca.it, March 2009

[6] S. Donatelli, E. Alata, A. Bondavalli, M. Beccuti, D. Cerotti, S. Chiaradonna, A. Daidone, G. Dondossola, F. Di Giandomenico, G. Franceschinis, F. Garrone, O. Hamouda, M. Kaâniche, P. Lollini, V. Nicomette, “Model-based evaluation of the middleware services and protocols & architectural patterns”, CRUTIAL Project, Work Package 5 - Deliverable D19, http://crutial.cesiricerca.it, March 2009

[7] G. Franceschinis, E. Alata, J. Antunes, H. Beitollahi, A. N. Bessani, M. Correira, W. Dantas, G. Deconinck, M. Kaâniche, N. Neves, V. Nicomette, P. Sousa, P. Verissimo, “Experimental validation of architectural solutions”, CRUTIAL Project, Work Package 5 - Deliverable D20, http://crutial.cesiricerca.it, March 2009

[8] F. Di Giandomenico, G. Deconinck, S. Donatelli, G. Dondossola, M. Kaậniche, P. Verissimo “Dissemination actions and collected publications”, CRUTIAL Project, Work Package 6 - Deliverable D21, http://crutial.cesiricerca.it, March 2009