



FP7-ICT-SEC-2007.1.7

Specific Targeted Research Project

225353

MICIE

Tool for systemic risk analysis and secure mediation of data
exchanged across linked CI information infrastructures

PERIODIC MANAGEMENT REPORT

Third Reporting Period

D1.3.2 – Final Management Report

Period covered: **from 01/05/2010 to 28/02/2011**

Date of preparation: **21/03/2011**

Start Date of Project: 01/09/2008

Duration: 30 months

Project Coordinator Name: Paolo Capodieci

Project Coordinator Organisation Name: Selex Communications S.p.A.

Revision: 0.9

DISCLAIMER

The work associated with this report has been carried out in accordance with the highest technical standards and the MICIE partners have endeavoured to achieve the degree of accuracy and reliability appropriate to the work in question. However since the partners have no control over the use to which the information contained within the report is to be put by any other party, any other such party shall be deemed to have satisfied itself as to the suitability and reliability of the information in relation to any particular use, purpose or application.

Under no circumstances will any of the partners, their servants, employees or agents accept any liability whatsoever arising out of any error or inaccuracy contained in this report (or any further consolidation, summary, publication or dissemination of the information contained within this report) and/or the connected work and disclaim all liability for any loss, damage, expenses, claims or infringement of third party rights.

CONTENTS

1	JUSTIFICATION OF MAJOR COST ITEMS AND RESOURCES.....	4
1.1	BRIEF DESCRIPTION OF WORK PERFORMED BY EACH CONTRACTOR	4
1.2	TABULAR OVERVIEW OF BUDGETED COST AND ACTUAL COSTS	16
1.3	TABULAR OVERVIEW OF BUDGETED PERSON-MONTHS AND ACTUAL PERSON-MONTHS	18
2	FORM C FINANCIAL STATEMENT PER ACTIVITY	19

1 JUSTIFICATION OF MAJOR COST ITEMS AND RESOURCES

1.1 Brief Description of Work Performed by each Contractor

Partner	WP No.	Description of task	p/m
SCOM	1	<i>Project Management</i> – Coordination of administrative and financial matter; Coordination of Internal Consortium Meetings; Management Information among EC and Partners. Monitoring of project activities. Financial Distribution. Preparation of all documentation required for the end of the Second Reporting Period and the associated Annual Review Meeting. Preparation and coordination of all documents for technical and administrative, for the end of project.	6.0
	2		
	3		
	4	Contribution on requirements identification and refinement of the requirements previously identified and reported in D4.1.2, with specific attention to the Secure Mediation Gateway and the ICT system interconnecting several Secure Mediation gateways. Detailed design of the logical architecture of the Secure Mediation Gateway reported in “D4.2.2 - Secure mediation gateway architecture - final version” including <ul style="list-style-type: none"> • revision of the use cases, • definition of the functionalities and their assembly into logical entities, • detailed functional architecture • definition of interactions among entities • definition of the activity diagrams • definition of the main interfaces at logical level, • definition of the database logical scheme. 	2.0
	5	The Software Design of the SMGW has been completed. Starting from the logical architecture defined in task 4003, the SMGW Communications Security modes have been defined, the Security Technology Stack has been selected and the design of the deployment architecture has been performed. Then the SMGW Data/Metadata DB has been designed and implemented using MySQL as RDBMS. Then using the structured O.M.G. methodology and the corresponding U.M.L. 2.0 tools the entities and macroentities that implement SMGW specific have been analyzed and designed, including <ul style="list-style-type: none"> • SMGW_admin • MetadataPublisher Web Service artifact • SMGWdaemon artifact • Remote Cisia Web Service • Adaptor Interface Web Service <p>The activity results are reported in “D5.2 - Secure Mediation Gateway SW Beta Release”</p>	7,5

Partner	WP No.	Description of task	p/m
		For an easier installation of the MICIE software a DVD with the MICIE distribution has also been realized. The DVD contains the operating system (Linux – Suse 11.3 distribution) with all those appliances required to run the SMGW, the wso2 middleware, as well as the MICIE Data base and the MICE applications. Distribution of MICIE SMGW software has been realized by means of SuseStudio. Full instructions on how to download and install the software are contained in the report “D5.2 - Secure Mediation Gateway SW Beta Release- Installation Guide”.	
	6	During the reporting period SCOM, in close cooperation with IEC and Roma Tre, has contributed to the implementation and setup of the system in Israel. The SMGW Demo system has been successfully integrated with the Adaptor and the Prediction Tool. Support to Itrust for penetration tests has also been given. SCOM has cooperated with FCTUC for the integration of the SMGW Policy-based Manager and the Trust and Reputation Service, and tests on the MICIE Demo System.	3.5
	7	Submission of the following papers: P. Simões, P. Capodieci, M. Minichino, E. Ciancamerla, S. Panzneri, M. Castrucci and L. Lev, “An Alerting System for Interdependent Critical Infrastructures,” Proc. of the 9th European Conference on Information Warfare and Security (ECIW 2010), Thessaloniki, Greece, 1-2 July 2010. Castrucci, Neri, Caldeira, Aubert, Khadraoui, Aubigny, Harpes, Suraci, “Design and implementation of a mediation system enabling secure communication among Critical Infrastructures”, Submitted to Elsevier International Journal of Critical Infrastructure Protection (IJCIP), February 2011 Capodieci, Neri, Castrucci, “Scambio di informazioni tra infrastrutture critiche”, Submitted to Safety and Security Italian Magazine, February 2011. Participation to “ICT event 2010”, Brussels, 27-29 September 2010, and contribution to the preparation of the material shown and distributed at the MICIE project stand. Participation to 2nd MICIE industrial workshop, Luxemburg, 20 May 2010. Participation to final MICIE workshop, Rome, 28 February 2011.	1.8
	Total		20.8
CRPHT	1	n/a	
	2	In this work package, CRPHT has enhanced the risk-based prediction methodology through the integration of the trust and reputation management defined by FCTUC. In parallel, the reference scenario defined within the deliverables D2.1.1 and D2.1.2 has been entirely instantiated using the methodology. Contribution to <ul style="list-style-type: none"> D2.1.2 – CI Reference Scenario and service oriented approach – final report D2.2.3 – Interdependency modelling framework, indicators and models – final report 	0
	3	In this work package, CRPHT has continued to refine the different components (taxonomy of assurance levels, security metrics and indicators) of the risk-based prediction methodology. Contribution to <ul style="list-style-type: none"> D3.2.2 – Common Ontology and Risk Prediction Algorithms – final version – in which the RESCI-MONITOR support tool is presented and its implementation detailed. 	5.99

Partner	WP No.	Description of task	p/m	
CRAT	4	In this work package, CRPHT has participated with CRAT, ROMA3, FCTUC and ITRUST, to the redaction of an article to be submitted at International Journal on Critical Infrastructure Protection (IJCIP). Contribution to <ul style="list-style-type: none"> D4.2.2 – Secure mediation gateway architecture – final version 	0.03	
	5	In this work package, CRPHT has <ul style="list-style-type: none"> Co-organized with ITRUST the M5 Consortium Internal Review Meeting and the 2nd MICIE Workshop – May 19-21, 2010. Presented a paper in ESREL 2010 Conference – Sept. 5-9, 2010. Participated to ICT 2010 event, Sept. 27-29, 2010. Submitted successfully and presented a paper in International Workshop on Risk and Trust in Extended Enterprises (RTEE'2010) – Nov. 1-4, 2010. Submitted successfully a paper in IST-Africa – May 11-13, 2011. Submitted unsuccessfully a paper with FCTUC at IEEE International Conference on Communications (ICC2011) – June 5-9, 2011. Submitted a paper with FCTUC at Fifth IFIP WG 11.11 International Conference on Trust Management – June 29-July 1, 2011. Submitted a paper at 41th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2011) – June 27-30, 2011. Participated with CRAT, ROMA3, FCTUC and ITRUST, to the redaction of an article to be submitted at International Journal on Critical Infrastructure Protection (IJCIP). Started to explore possibilities to adapt the RESCI-MONITOR approach to other sectors (financial and transports, among others) and to other purposes (e.g. for crisis management). Presented the RESCI-MONITOR approach and the associated tool at the MICIE Final Workshop held in Rome – Feb. 28, 2011. Contribution to <ul style="list-style-type: none"> D7.1.3 – Dissemination and Exploitation – Final Report – in which all the dissemination and exploitation activities have been presented. 	3.74	
	6		Total	16.25
	7			
				Total
	1	N/A		

Partner	WP No.	Description of task	p/m
	2	<p>During the third reporting period CRAT has finalized the research on the modelling of CI-interdependencies, by using dynamic bayesian belief network.</p> <p>Activities have been carried on as follows:</p> <ul style="list-style-type: none"> • Refinement of static model (BN) on the basis of further information received by IEC. • Design of the dynamic model (DBN) based on the analysis of temporal dependencies among devices, functionalities and services. • Simulations of realistic scenarios on the final DBN. <p>The designed model is able to evaluate the status of the following services:</p> <ul style="list-style-type: none"> • Power Supply to Final MV customers • Remote Control of MV Disconnectors <p>The designed model allows to perform the following analyses:</p> <ul style="list-style-type: none"> • Reliability analysis: To calculate the probability $R(t)$ that any of the CI's services will operate without failure up to time t, under standard operational conditions; • Adverse events propagation and prognosis: To evaluate the impact of adverse events on services, recognizing and preventing possible degradation of services; • Diagnosis: To establish a causal connection between a failure, its possible causes and its consequences. <p>All the work done is detailed in the contribution provided for D2.2.3 "Interdependency modelling framework, indicators and models - final report".</p>	
	3	<p>Starting from the Entity-Relations schema produced in the previous reporting period, CRAT extended the ontology model already presented in D4.2.1, in order to include in the model also the new entities and the new relationships appeared in the E-R diagram.</p> <p>Thus, the final E-R schema has been designed in order to include all the elements and the relationships among them that are relevant for the scenarios considered in the MICIE project.</p> <p>This updated E-R schema has been also used as the basis to produce the final ontology able to provide a common and CI independent view of the system.</p> <p>The work done has been reported in Deliverable D3.2.2 "Common ontology and risk prediction algorithms – final version".</p>	

Partner	WP No.	Description of task	p/m
	4	<p>As WP4000 leader, during this reporting period, CRAT performed the coordination of all the activities performed within WP4000.</p> <p>CRAT performed a revision of the ER schema and the ontology already developed in the previous part of the project.</p> <p>In particular, starting from the updated information about the modeling activities from WP3000, CRAT developed a new ER schema and translated it into an OWL schema using the Protégé tool. In addition, several examples of OWL instances for the Electrical CI and the Telecommunication CI has been created.</p> <p>Moreover, on the basis of the test results obtained during the second reporting period, during which the UPnP/Open VPN and the web service based information discovery and sharing approaches were compared, CRAT developed, together with other partners of the consortium, a Web service based solution for information discovery in a cooperative CI environment, taking into consideration possible undisclosed constraints.</p> <p>In addition, starting from the preliminary results about the design of the SMGW architecture, a more detailed architecture has been developed in cooperation with other partners.</p> <p>CRAT also realized several UML diagrams to describe the functional structure and the behavior of the SMGW and of some of its elements. For example, the following figures describes Message sequence chart diagrams in case of pull or push mechanisms applied for information sharing in the SMGW.</p> <p>Detailed description of the defined ontology, the SMGW architecture and its formal documentation realized using UML diagrams was reported in D4.2.2 "SMGW architecture – final version"</p>	
	5	<p>CRAT designed, implemented, tested and integrated a Service Discovery feature to be included in the SMGW realized in WP5000.</p> <p>In particular, in the context of the MICIE project, the Discovery procedure is required when a new Critical Infrastructure joins the MICIE network. The objective of this procedure is to share a proper sub-set of CI's information throughout the network. Not all the CIs, in fact, have the same confidence between themselves. We can imagine a scenario in which, for example, CI A and CI B are managed by two companies that are allied with each other, while CI C is managed by a company that has no relationship with the others. In this context is evident that not all data have to be shared throughout the network but only a proper sub-set of data, depending on a sort of confidence level between CIs.</p> <p>In order to guarantee sensible data protection, a new algorithm has been designed and developed by CRAT. The proposed algorithm is an enhanced Bron-Kerbosch algorithm. It has been developed in order to build the federation graph among heterogeneous CIs.</p> <p>Once realized the algorithm, CRAT integrated it into the MICIE context. In particular a Web Service has been realized in JAVA under the WSo2 framework, in order to be compliant with the SMGW implementation. In particular a JAVA client has been developed, compliant with the JSPs (JavaServer Pages) of the SMGW provided by SCOM. The Client will interact with a Web Service Server, realized by CRAT, which performs the developed algorithm throughout the MICIE network. After the execution of the algorithm, the Web Service Server will send e result to the JAVA Client realized by CRAT. This JAVA Client will interact with the existing (and update with the algorithm needed information) Database provided by SCOM by means of SQL queries in order to transparently integrate itself with the SMGW functionalities already realized by the WP5000 team.</p>	
	6	N/A	

Partner	WP No.	Description of task	p/m
	7	<p>Submission of the following papers:</p> <p>P. Simões, P. Capodiecì, M. Minichino, E. Ciancamerla, S. Panzìeri, M. Castrucci and L. Lev, "An Alerting System for Interdependent Critical Infrastructures," Proc. of the 9th European Conference on Information Warfare and Security (ECIW 2010), Thessaloniki, Greece, 1-2 July 2010</p> <p>Aubigny, Harpes, Castrucci, "Risk ontology and Service Quality Descriptor shared among interdependent Critical Infrastructures", 5th International Conference on Critical Infrastructures Security, CRITIS 2010, 23-24 September 2010, Athens, Greece</p> <p>Di Giorgio A., Liberati F., "A Bayesian Belief Network Approach to the Critical Infrastructure Interdependencies Analysis", submitted to IEEE Systems Journal, special Issue "Complexity in Engineering: from Complex Systems Science to Complex Systems Technology", October 2010</p> <p>Di Giorgio A., Liberati F., "A Dynamic Bayesian Network Based Approach to the Critical Infrastructure Interdependencies Analysis", submitted to the Mediterranean Conference on Control and Automation MED 2011</p> <p>Castrucci, Neri, Caldeira, Aubert, Khadraoui, Aubigny, Harpes, Suraci, "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures", Submitted to Elsevier International Journal of Critical Infrastructure Protection (IJCIP), February 2011</p> <p>Capodiecì, Neri, Castrucci, "Scambio di informazioni tra infrastrutture critiche", Submitted to Safety and Security Italian Magazine, February 2011.</p> <p>Participation to "Future Network & Mobile Summit 2010", Florence, 16-18 June 2010, and presentation of the following MICIE paper during a poster session: "Secure Mediation Gateway Architecture Enabling the Communication Among Critical Infrastructures".</p> <p>Participation to "ICT event 2010", Brussels, 27-29 September 2010, and contribution to the preparation of the material shown and distributed at the MICIE project stand.</p> <p>Participation to 2nd MICIE industrial workshop, Luxemburg, 20 May 2010.</p> <p>Participation to final MICIE workshop, Rome, 28 February 2011.</p> <p>Contributions to the MICIE web-site contents, adding news and events.</p> <p>Teaching activities made during the courses provided at "La Sapienza" University of Rome to both Master students and PhD students, where topics related to MICIE project has been presented together with some project results and achievements. In addition several master thesis took advantage of the MICIE research activities, as several students had the opportunity to work in MICIE related research issues.</p> <p>CRAT contributed to the Deliverable D7.1.3 "Dissemination and Exploitation, Final Report".</p>	
		Total	
ROMA3	1		
	2	Gathering and refinement of the comprehension of reference scenario, by means of technical meetings in Israel and close cooperation with IEC and ENEA.	3.43
	3	Implementation of the Model within CISIA framework.	3.79
	4	Refinement of MHR model with respect to the reference scenario. Close cooperation with IEC in order to represent properly the scenario and to provide adequate provisions on the state of the system and, in particular, of the FISR service.	1.36
	5	Implementation of the online prediction tool architecture, in close cooperation with IEC and Selex COM. In particular the web services adopted have been designed, as well as the Human-Machine Interface used to present the results to the operators.	2.31
	6	Testing and setup of the online system in Israel	0.5

Partner	WP No.	Description of task	p/m
	7	Management and preparation of the MICIE final meeting held in Rome, 28 February 2011.	0.67
		Total	12.06
ENEA	1		
	2	<p>Final refinement of reference scenario, identification of services and refinement of interdependency models have been performed. Regarding to reference scenario, services have been identified as the procedures that the operators of the Telco Control Centre and SCADA control Centre perform to manage the Telco network and the power grid under nominal conditions and adverse events, according to motivated service selection criteria. A major effort has been spent on the Telco network and procedures to be performed by the operator of the Telco Control Centre in normal service operation, incident, and emergency and crisis situations. Regarding to heterogeneous models refinement, several aspects has been taken into account: a) demonstration of traceability of models against the reference scenario and reference networks currently available; b) careful identification of actual model inputs and outputs; c) clear identification of model expected outputs; d) real time capability of models to assist on line SCADA and NMS operators. Particularly, models afford the <i>quality of the service to grid customers</i> related to the risk of loss/degradation of <i>Fault Isolation and System Restoration (FISR)</i> service, including security aspects, as a benchmark for the various modelling approaches. Among others:</p> <ul style="list-style-type: none"> – Dynamic Bayesian Belief Networks (DBNs) to take time into account have been implemented. – Refinements of Deterministic and agent based simulation (RAO) model to fully represent reference scenario and demonstrations of running on line RAO model have been performed. – RESCI-MONITOR (Real-time Evaluation of Security – MONITOR) has been improved and demonstrations of running on line model have been performed. – Refinements of NS2 models to performs QoS computation of FISR service, in terms of reliability indexes (S-T connectivity: minpaths, mincuts and reliability), performances indexes (time response, % of affected customers, RTT and dynamical paths) and demonstrations of running model have been performed. 	3.0

Partner	WP No.	Description of task	p/m
	3	<p>A detailed guideline to compare the modelling approaches, the models and the results developed within WP2000, has been provided, as contribute to select /integrate models for risk prediction tool. Modelling approaches can be analysed and compared with the final aim to give hints to WP3000 in terms of knowledge, indicators, and model adequacy to be ideally integrated and fit into the development cycle of on line risk prediction tool.</p> <p>Service selection criteria have been proposed to allow building models able to perform a (relatively quick) interdependency analysis. Then, as services we mean predefined operations carried out under the real events or alarms received from the CI, by SCADA and by NMS operative and maintenance personnel. The selected operative and maintenance procedures of SCADA operator were:</p> <ul style="list-style-type: none"> – "22 KV Medium Voltage Grid Fault Location, Isolation and Restoration" procedure (FISR) – Recovery from Remote Terminal Unit (RTU) failures; – RTU maintenance procedures. <p>Such procedures should account the occurrence of adverse events from other infrastructures and:</p> <ul style="list-style-type: none"> – VHF Communication disturbances; – Failure of the RTU equipment, including power supply and batteries; – Power supply loss <p>The selected operative and maintenance procedures of NMS operator were:</p> <ul style="list-style-type: none"> – Recovery from failures; – Maintenance of the SDHs; – Data collection procedure and some metrics. <p>Such procedures should account the occurrence of adverse events from other infrastructures and:</p> <ul style="list-style-type: none"> – Communication disturbances; – Failure of the SDH equipment (including power supply and batteries). 	1.6
	4	<p>ENEA has contributed to functional requirement of Risk prediction tool. The focus was on the service delivered by interconnected infrastructures. The interdependency indicators may change according to the selected service. The selection of adequate interdependency indicators should feed the criteria of identification of functional requirement of risk prediction tool. Among such interdependency indicators, focusing on FISR service, the following indicators have been discussed and proposed:</p> <ul style="list-style-type: none"> – Response time of FISR time as a composed indicator of FISR. FISR response time is referred here as a composed indicator because it depends upon the values of indicators of reliability and performances of the networks that support such a service, here referred as basic indicators. 	0.9
	5		

Partner	WP No.	Description of task	p/m
	6	Validation activities have been based on the validation scenario derived from the final reference scenario as described in deliverable D2.1.2. ENEA has mainly contributed to the identification of expected results and the validation procedures. Practically, four types of validation tests of MICIE Alerting system with focus on Fault Isolation and System Restoration procedure (FISR) have been identified within the IEC Simulation Test Bench (STB): <ul style="list-style-type: none"> - interactive validation tests, that test the human system interface; - integration validation tests, that perform the tests already performed on MICIE alerting system as isolated system, on MICIE alerting system integrated into the validation environment - dynamic validation tests, that test MICIE alerting system with respect to the execution of FISR procedure under different operational scenarios. - penetration validation tests, which address security and trustworthy of MICIE Alerting system 	3.0
	7	Submission and presentation of several papers in international conferences as reported in to D7.1.3 "Dissemination and Exploitation, Final Report"; Contributions to MICIE workshops Contributions to D7.1.3 "Dissemination and Exploitation, Final Report".	1.9
	Total		10.4
PIAP	1		
	2		
	3	Development and tests of aggregation module for further use in Adaptor	0.3
	4	Definition of the model of specialized interface/adaptor connection to the SMGW together with CI (Structure of Adaptor and Guidelines for adaptor implementations).	2,1
	5	Development and tests of adaptable and scalable Adaptor for connection to the CI, the LabVIEW environment has been selected for the implementation of the requirements together with the technological aspects.	3.6
	6	The MICIE Adaptor software for communication with Wizcon SCADA as data source was deployed on a local machine and configured. The MICIE LightSoft Connectivity Software for communication with LightSoft NMS was deployed on a local machine and configured.	15.2
	7		
	Total		21.2
IEC	1		
	2		
	3		
	4		
	5		
	6	IEC finished test of the Simulation Test Bench (STB) for validation of the MICIE Tool. IEC designed validation procedures for the validation of the MICIE Tool. IEC implemented integration of the STB, Adaptors and MICIE Tool. The MICIE Tool validation was passed successfully and the results were published in the D6.3 document "validation Activity Report". The D.3 document "Validation Activity Report" was prepared.	10.6
	7	IEC contributed to the papers published during the 3rd Period. IEC presented MICIE project at the EUTC2010 conference in London, October2010. IEC presented the results of the WP6 during the Workshop in Rome, February 2011.	0.3
	Total		10.9
IIRUSE	1		
	2		

Partner	WP No.	Description of task	p/m
	3	In this work package, Itrust has continued to work on the refinement of the risk-based methodology especially on the security model according to a QoS degradation approach based on the dependability concept and a similar approach as ISO 15408. A presentation and a poster for the CRITIS conference have been prepared. NB: the workload in this period was 0,4, the indicated value compensated for a reporting error in the previous period.	0.1
	4	In this work package, Itrust has refined the Protection Profile of the SMGW communication agent proposed in the D4.2.1 report according to the Common Criteria framework. The Protection Profile has been completed by the specifications of the Security Functional Requirements. The proposed SMGW requirements defined in the report D4.2.1 has been analyzed according to the SFR. A poster for the conference SRC'10 has been prepared. ITRUST has also refined and supplemented the D4.2.2 report changed according to the Project Officers feedback.	0.1
	5		0
	6	Itrust installed and tested the SMGW developed by SELEX. A set of penetration was executed and the result described in a specific report. The software application has been tested according to the OWASP methodology (seven tests of OWASP testing), specific PenTest tool - e.g. open Vas, Grendel Sscan, Zenmap, and the software code has been studied to identify potential weaknesses. No significant weaknesses have been identified, but some recommendations for a potential operator have been formulated.	0.9
	7	Itrust has organised the MICIE application workshop in Luxembourg on 20 th May and the internal review on May 19 th and 21 st , in collaboration with the CRP Henry Tudor. Itrust was in charge of the technical program, identified speakers and discussed all draft presentation with the authors and moderated the conference panel discussion. Press releases have been prepared, and itrust made an article for the journal "Revue technique" of the engineering association, and gave an interview for a technical article in the journal "Letzebuenger Gemengen". Itrust submitted and presented a paper on the risk level assessment methodology based on dependability concept to the CRITIS 2010 Conference in Athen. The paper has been retained for the poster session and a shorter version was finalised. Itrust has also submitted a paper and a poster on the Protection Profile of the SMGW communication agent, and assisted to the SRC10 conference in Oostende. Itrust has also participated to the ICT days in Brussels to present the MICIE project and to prospect future opportunities for the MICIE tools. Itrust presented the general finding of the MICIE project about the Power Grid, Telco networks management to a Luxembourg consortium in the framework of research project led by the Luxembourg Research Ministry. This presentation allowed defining which type of business opportunities for Satellite Telecommunication Solution in Energy Sector. Itrust has also participated to writing of the MICIE journal paper on the MICIE Secure Mediation Gateway. Itrust presented its own contribution to MICIE project in the last workshop in Rome.	2.5
Total			3.6
MULT	1	N/A	
	2	No activities for the period	
	3	N/A	
	4	N/A	
	5	N/A	
	6	An on-line version of simulation model, including communication protocol with external software, has been tested to verify the communication module work.	0.3

Partner	WP No.	Description of task	p/m
	7	Preparation and participation in ICT'2010 Redaction and presentation of scientific paper on International Congress on intelligent systems and information technologies AIS-IT 2010 Preparation and participation in MICIE final Workshop	0.2
		Total	0.5
FCTUC	1	N/A	-
	2	FCTUC continued with the study of scenarios and service-oriented approaches for critical infrastructures, including the research of trust-based input for the MICIE models. More specifically, a trust-based add-on to the MICIE Framework was proposed and integrated with the risk-based prediction methodology previously proposed by CRPHT. FCTUC also contributed to the following WP2000 deliverables: D2.2.2 (Interdependency modeling framework and interdependency indicators and models (interim)), D2.2.3 (Interdependency modeling framework and interdependency indicators and models (Final)), and D2.1.2 (CI Reference Scenario and service oriented approach (Final Report))	0.58
	3	FCTUC focused WP3000 work on tools to evaluate hidden dependencies, and on ontologies and methods to exchange data with the field and feed the interdependency on-line evaluator. FCTUC also worked on the inclusion of trust models in the MICIE risk prediction algorithms and contributed to Deliverable D3.2.2 (Common ontology and risk prediction algorithms – final version).	0.70
	4	FCTUC focused its WP4000 activities on the following topics: - Refinements of the MICIE SMGW, including its SOA architecture. - Refinements of the SMGW Cross Domain Communication System. - Management of the MICIE SMGW, by means of a policy-based management service. - Extensions with an optional Trust and Reputation Service. FCTUC participated in the preparation of several research papers directly related to the work performed in the scope of WP4000 (Security, Trust Models, Policy-based Management) and contributed to Deliverables D4.1.2 (MICIE ICT system requirements - final version) and D4.2.2 (Secure Mediation Gateway Architecture - final version).	0.58
	5	FCTUC participated in the development of the MICIE platform (SMGW components), namely providing the Trust and Reputation System and the Policy-based SMGW Manager previously conceived in WP4000. FCTUC also participated in preliminary integration activities related with these two SMGW components. FCTUC also contributed to Deliverable D5.2 (Secure Mediation Gateway SW Beta Release).	2.75
	6	FCTUC performed the integration of the SMGW Policy-based Manager and the Trust and Reputation Service on the MICIE Demo System provided by IEC, with off-site and on-site tests (integration and functional tests). FCTUC also performed complementing validation studies, by simulation and emulation, in order to evaluate these two components in a number of hypothetical scenarios. FCTUC contributed to Deliverables D6.1 (Demonstration Plan), D6.2 (Integration Process Report) and D6.3 (Validation Activities), focused on the validation of the previously developed SMGW modules (both integrated functional validation and generic validation studies supported by simulation) and on the general security aspects of the SMGW.	3.25

Partner	WP No.	Description of task	p/m
	7	FCTUC, as Leader of WP7000, performed the following tasks: - Preparation of D7.1.3 (Dissemination and Exploitation – Final Report). - Preparation of and participation in the Luxembourg workshop (May 2010). - Preparation of and participation in the Rome workshop (February 2010). - Organization of the ICT 2010 exhibition stand. - Organization of the ServiceWave 2010 exhibition stand. - Presentation and publication of 7 MICIE papers (conferences, journals) - Preparation and submission of 2 MICIE papers (pending review). - Presentation of the MICIE Project at the following events: “SMART ENERGY Brainstorms: R&D for the Future of Smart Energy Grids: fostering pilot experiences in Portugal” (Lisbon, June 15th, 2010); NET-SCIP Workshop on Security (Porto, October 13th, 2010); “Ciência 2010 – Encontro com a Ciência e a Tecnologia em Portugal” (July 5th 2010). - Enhancement and maintenance of the project’s web portal. - Preparation of a draft proposal for a book based on MICIE research.	1.90
	Total		9.76
INIBRAD	1		
	2		0.2
	3	Our main research efforts focused on DBN models: - Structure learning combined with multi-dimensional Gaussian observation nodes. Improvement of the modelling of a class with respect to other classes. - Optimisation of the sequences of observation, via Evolutionary Algorithm and a hierarchical Bayesian classifier. - Introduction of the “Multiscale DBN”, to investigate interdependencies into several scales of the data. - Use of shape descriptor features as input for the DBN	8.6
	4		
	5		
	6		
	7	5 papers have been written.	1.4
	Total		10.2

1.2 Tabular Overview of Budgeted Cost and Actual Costs

See on Next Page

Cost Budget Follow-Up Table								
Contract No.: 225353		Project Acronym: MICIE					Date: 21/03/2011	
Partner Acronym	Type of Expenditure	Budget	Actual Costs (€)				% spent	Remaining Budget (€)
			Period 1	Period 2	Period 3	Total		
SCOM	Total person-month	48	1,40	23,30	22,20	46,90	97,7%	1,10
	RTD/Innovation	435.400,00	0,00	186.447,29	206.460,96	392.908,25	90,2%	42.491,75
	Demonstration	38.700,00	0,00		38.530,71	38.530,71	99,6%	169,29
	Management	250.320,00	14.365,00	80.861,87	111.605,97	206.832,84	82,6%	43.487,16
	Other costs		0,00			0,00	0,0%	0,00
	Total Costs	724.420,00	14.365,00	267.309,16	356.597,64	638.271,80	88,1%	86.148,20
CRPHT	Total person-month	26	7,30	10,98	16,25	34,54	132,8%	-8,54
	RTD/Innovation	294.880,00	67.806,42	97.574,64	124.732,77	290.113,83	98,4%	4.766,17
	Demonstration					0,00	0,0%	0,00
	Management					0,00	0,0%	0,00
	Other costs					0,00	0,0%	0,00
	Total Costs	294.880,00	67.806,42	97.574,64	124.732,77	290.113,83	98,4%	4.766,17
CRAT	Total person-month	32	13,00	21,20	12,80	47,00	146,9%	-15,00
	RTD/Innovation	365.332,00	124.995,45	191.254,89	150.208,55	466.458,89	121,1%	-81.126,89
	Demonstration					0,00	0,0%	0,00
	Management					0,00	0,0%	0,00
	Other costs					0,00	0,0%	0,00
	Total Costs	365.332,00	124.995,45	191.254,89	150.208,55	466.458,89	121,1%	-81.126,89
ROMA3	Total person-month	59	20,12	27,32	12,06	59,50	100,8%	-0,50
	RTD/Innovation	345.881,60	124.240,71	163.618,57	67.746,13	365.605,41	102,8%	-9.723,81
	Demonstration					0,00	0,0%	0,00
	Management				4.644,21	4.644,21	0,0%	-4.644,21
	Other costs	19.200,00			22.027,22	22.027,22	114,7%	-2.827,22
	Total Costs	365.081,60	124.240,71	163.618,57	94.417,56	362.276,84	104,7%	-17.195,24
ENEA	Total person-month	35	12,00	12,60	10,40	35,00	100,0%	0,00
	RTD/Innovation	397.665,00	129.746,00	137.980,92	130.500,00	398.226,92	100,1%	-561,92
	Demonstration					0,00	0,0%	0,00
	Management					0,00	0,0%	0,00
	Other costs					0,00	0,0%	0,00
	Total Costs	397.665,00	129.746,00	137.980,92	130.500,00	398.226,92	100,1%	-561,92
PIAP	Total person-month	21	2,60	9,20	21,20	33,00	157,1%	-12,00
	RTD/Innovation	159.212,00	14.890,15	36.856,06	108.459,17	160.205,38	100,6%	-993,38
	Demonstration					0,00	0,0%	0,00
	Management					0,00	0,0%	0,00
	Other costs					0,00	0,0%	0,00
	Total Costs	159.212,00	14.890,15	36.856,06	108.459,17	160.205,38	100,6%	-993,38
IEC	Total person-month	26	7,00	9,10	10,90	27,00	103,8%	-1,00
	RTD/Innovation	433.890,00	109.651,00	144.249,00	184.000,00	437.900,00	100,9%	-4.010,00
	Demonstration					0,00	0,0%	0,00
	Management					0,00	0,0%	0,00
	Other costs					0,00	0,0%	0,00
	Total Costs	433.890,00	109.651,00	144.249,00	184.000,00	437.900,00	100,9%	-4.010,00
ITRUST	Total person-month	15	5	11	3,60	18,84	125,6%	-3,84
	RTD/Innovation	124.557,00	37.825,00	56.797,00	52.737,00	147.359,00	118,3%	-22.802,00
	Demonstration	8.219,00	0,00		9.363,20	9.363,20	113,9%	-1.144,20
	Management		0,00			0,00	0,0%	0,00
	Other costs		0,00			0,00	0,0%	0,00
	Total Costs	132.776,00	37.825,00	56.797,00	62.100,20	156.722,20	118,0%	-23.946,20
MULT	Total person-month	19	7,42	12,4	0,52	20,30	106,8%	-1,30
	RTD/Innovation	216.000,00	85.086,89	144.766,43	15.171,72	245.025,04	113,4%	-29.025,04
	Demonstration					0,00	0,0%	0,00
	Management					0,00	0,0%	0,00
	Other costs					0,00	0,0%	0,00
	Total Costs	216.000,00	85.086,89	144.766,43	15.171,72	245.025,04	113,4%	-29.025,04
FCTUC	Total person-month	17	3,10	7,40	9,80	20,30	119,4%	-3,30
	RTD/Innovation	206.400,00	33.465,00	108.372,00	83.070,40	224.907,40	109,0%	-18.507,40
	Demonstration					0,00	0,0%	0,00
	Management					0,00	0,0%	0,00
	Other costs				29.444,00	29.444,00	0,0%	-29.444,00
	Total Costs	206.400,00	33.465,00	108.372,00	112.514,40	254.351,40	123,2%	-47.951,40
UNIBRAD	Total person-month	16	3,60	17,80	10,20	31,60	197,5%	-15,60
	RTD/Innovation	180.800,00	20.545,00	37.300,00	44.200,00	102.045,00	56,4%	78.755,00
	Demonstration					0,00	0,0%	0,00
	Management					0,00	0,0%	0,00
	Other costs					0,00	0,0%	0,00
	Total Costs	180.800,00	20.545,00	37.300,00	44.200,00	102.045,00	56,4%	78.755,00
TOTAL	Total person-month	314	82,28	161,76	129,93	373,98	119,1%	-59,98
	RTD/Innovation	3.180.017,60	748.251,61	1.305.216,80	1.167.286,70	3.220.755,11	101,3%	-40.737,51
	Demonstration	46.919,00	0,00		0,00	47.893,91	102,1%	-974,91
	Management	250.320,00	14.365,00	80.861,87	116.250,18	211.477,05	84,5%	38.842,95
	Other costs	19.200,00	0,00	0,00	51.471,22	51.471,22	268,1%	-32.271,22
	Total Costs	3.496.456,60	762.616,61	1.386.078,67	1.382.902,01	3.531.597,29	101,0%	-35.140,69

1.3 Tabular Overview of Budgeted person-months and Actual person-months

Person-Month Status Table			Partner - Person-month per Workpackage												
CONTRACT N°:	225353														
ACRONYM:	MICIE														
PERIOD:	1/05/2010 to 28/02/2011		TOTALS	SCOM	CRPHT	CRAT	ROMA3	ENEA	PIAP	IEC	ITRUST	MULT	FCTUC	UMBRAD	
Workpackage 1000:	Project Management	Actual WP total:	6	6,0											
		Planned WP total:	14	14,0											
Workpackage 2000:	Interdependency Analysis and Modelling	Actual WP total:	8,1	0,0	0,0	0,8	3,4	3,0	0,0	0,0	0,0	0,0	0,58	0,2	
		Planned WP total:	68	2,0	2,0	6,0	12,0	23,0	0,0	4,0	3,0	12,0	2,0	2,0	
Workpackage 3000:	Risk prediction system design	Actual WP total:	21,8	0,0	6,0	0,7	3,8	1,60	0,3	0,0	0,1	0,0	0,70	8,6	
		Planned WP total:	68	0,0	7,0	4,0	36,0	4,00	4,0	0,0	5,0	0,0	2,0	6,0	
Workpackage 4000:	Mediation system design	Actual WP total:	8,8	2,0	0,0	1,7	1,4	0,90	2,1	0,0	0,1	0,0	0,58	0,0	
		Planned WP total:	45	7,0	8,0	12,0	6,0	2,00	0,0	2,0	3,0	3,0	2,0	0,0	
Workpackage 5000:	Development of on-line risk prediction tool and Secure Mediation GW	Actual WP total:	31,28	7,5	6,5	8,6	2,3	0,00	3,6	0,0	0,0	0,0	2,75	0,0	
		Planned WP total:	51	18,0	5,0	7,0	3,0	0,00	5,0	3,0	0,0	0,0	5,0	5,0	
Workpackage 6000:	Validation	Actual WP total:	37,24154	3,5	0,0	0,0	0,5	3,00	15,2	10,6	0,9	0,3	3,25	0,0	
		Planned WP total:	42	4,0	0,0	0,0	0,0	3,00	12,0	15,0	2,0	1,0	3,0	2,0	
Workpackage 7000:	Dissemination & Exploitation	Actual WP total:	15,4	1,8	3,7	1,0	0,7	1,9	0,0	0,3	2,5	0,2	1,90	1,4	
		Planned WP total:	26	3,0	4,0	3,0	2,0	3,0	0,0	2,0	2,0	3,0	3,0	1,0	
		Actual total:	128,5	20,8	16,3	12,8	12,1	10,4	21,2	10,9	3,6	0,5	9,8	10,2	
Total Project Person-month		Planned total:	314,0	48,0	26,0	32,0	59,0	35,0	21,0	26,0	15,0	19,0	17,0	16,0	

2 FORM C FINANCIAL STATEMENT PER ACTIVITY

Form C will be provided after the compilation on NEF Tool

End of Document