SIXTH FRAMEWORK PROGRAMME
PRIORITY 2
"Information Society Technologies"

Project acronym: DESEREC
Project full title: Dependability and Security by Enhanced Reconfigurability
Proposal/Contract no.: IST-2004-026600-DESEREC

D5.4
Plan for Using and Disseminating Knowledge

Project Document Number: DESEREC/D5.4/PU[1]/v1.0
Project Document Date: 13/07/2007
Workpackage Contributing to the Project Document: WP5
Deliverable Type and Security: R[2]-PU
Author(s): Luca Durante (IEIIT)

Abstract:
This document provides a report on the past and planned dissemination and exploitation activities.

Keywords: dissemination, exploitation

[1] Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

[2] Type: P - Prototype, R - Report, D - Demonstrator, O - Other

History

Version	Date	Description, Author(s), Reviser(s)
1.0	13/07/2007	PMT approved version, Luca DURANTE, Manuel CHEMINOD

Executive Summary

This document provides a report on the dissemination activities related to the DESEREC project.

This report focuses both on past activities and on future planned activities. In DESEREC several lines and ways for dissemination have been selected, and for each one the current status and the foreseen actions are depicted.

Dissemination activities are:

- Managing the project web site making available all public materials and advertising about project related events
- Producing regular project newsletter introducing key achievements
- Organising dissemination workshop and publishing its materials
- Reporting about project-related publications and conference participations

Contents

Page

1 Introduction 5

2 Foils & leaflets, partners' description 6

3 Web site 8

4 Newsletter 9
4.1 Newsletter Past Issues 9
4.1.1 October 2006 9
4.1.2 July 2007 9
4.2 Future Issues 9

5 Papers and Presentations 10
5.1 Published and submitted papers 10
5.1.1 Published papers 10
5.1.2 Submitted papers 11
5.2 Presentations 11
5.3 Publication plan 12
5.3.1 POLITO 12
5.3.2 UMU 12
5.3.3 IEIIT 12
5.3.4 ENST 13
5.3.5 BUTE 13
5.3.6 PWR 14

6 Workshops and Conferences 15
6.1 Conferences 15
6.2 Workshops 15
6.2.1 1st Training Workshop 15
6.2.2 1st Dissemination Workshop 16
6.3 Planned activities 17
6.3.1 2nd Training Workshop 17
6.3.2 2nd Dissemination Workshop 17
6.3.3 3rd Training Workshop 18

7 Exploitation Plan 19

Figures, Tables

Figure 1: DESEREC Leaflet 6
Figure 2: Thales partner description on web site 7
Figure 3: The DESEREC web site 8

Table 1 : Disseminaton lines 5

1 Introduction

The dissemination activities related to the DESEREC project aim at presenting the project results to a heterogeneous audience, ranging from private and public organizations, industries, to academia and research institutions; and from security and dependability professionals to a larger community of potential users.

Three main ways for distributing results are exploited:

- workshops and conferences organization or co-organization by DESEREC
- papers publications on journals and conferences proceedings and presentations to workshops and conferences
- internet/web dissemination and newsletter distribution

We can feature the main dissemination lines with respect to expected audience, as reported in Table 1:

- foils & leaflets, partners' description
- web site
- newsletter
- papers and presentations
- workshops and related material : workshops/conferences (co)organization as well as scientific publications and presentations

Each point will be further described in the next sections.

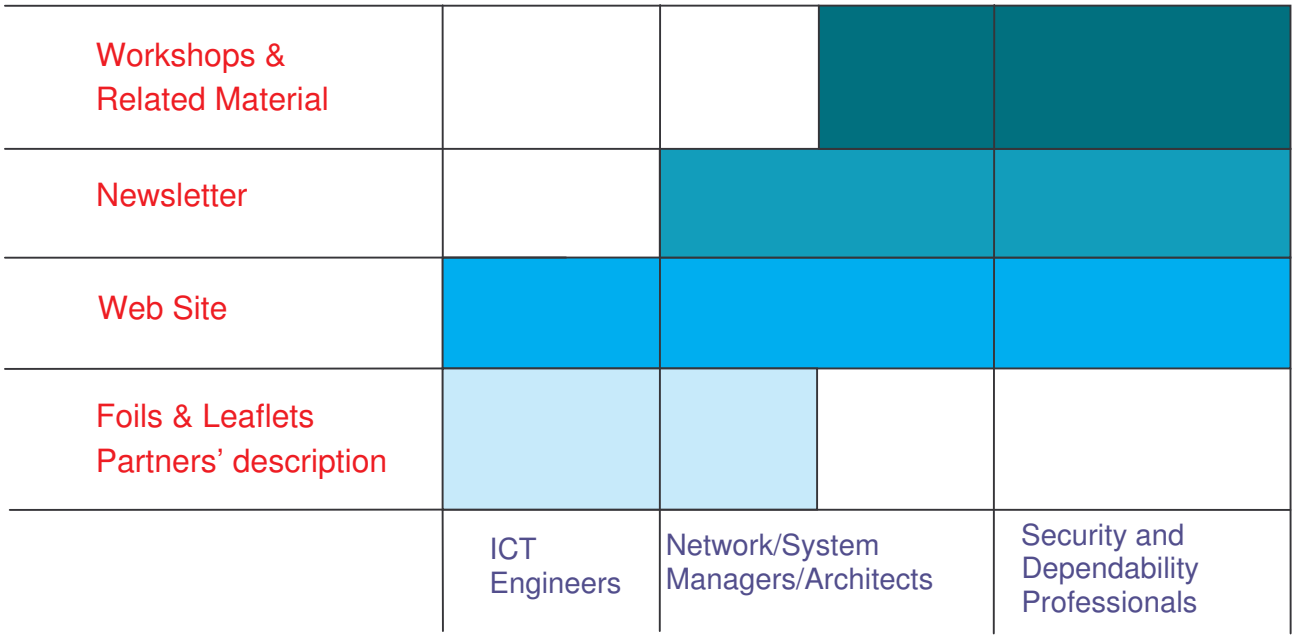

Table 1 : Disseminaton lines

2 Foils & leaflets, partners' description

Foils & leaflets targeting unskilled people have been prepared.

Partners' descriptions have been gathered in the DESEREC web site, featuring partners' profile and their involvement in the project as well as their exploitation plan.

Foils and leaflets are available on the web site, and have been used to build the project description on the web site, in order to provide homogeneous descriptions on heterogeneous media.

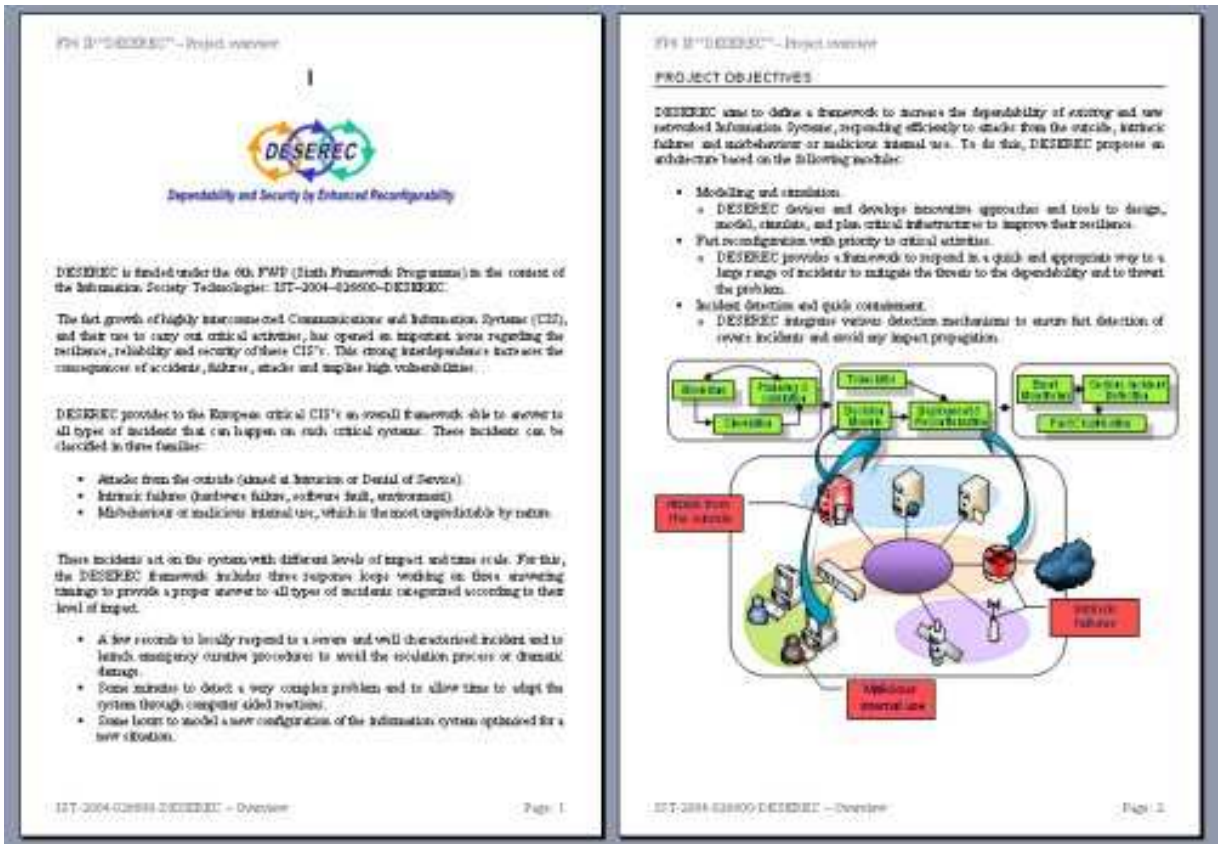

Figure 1: DESEREC Leaflet

The same approach has been followed for the partners' descriptions: on this basis the partners' pages on the web site have been designed.

For instance, figure 3 shows how the Thales description page does look.

THALES

Company Profile

The Thales Architecture Framework (TAF) is an horizontal entity across the Thales Group (60,000 people - over €10 bn revenues) , in charge of devising common architectures/frameworks. The TAI laboratory involved in Deserec, feeds TAF with the mid-term technology:

- develop/evaluate software components for Security, Wireless/ad hoc networks, Multimedia.
- design/implement the candidate architecture for mission-critical networked systems and applications, Resilience and availability, Security, Deployment and reconfiguration

Contact Information

www.thalesgroup.com
André Cotton : E-Mail

Involvement in Deserec

Thales is the DESEREC leader, coordinating the project and also providing expertise and tools in the following areas:

- Overall architecture
- Planned and hot reconfiguration; policies for reconfiguration
- Apply data analysis technology to incident early detection and isolation scope
- Overall reconfiguration concepts; I.S. Modelling
- Detection of complex intrusion scheme

Company exploitation plan

Exploitation and dissemination plan will include:

- Improve expertise in managing the resilience of services within large and complex information systems
- Distribution of DESEREC key advantages within Thales group
- Improve the design of future I.S. solutions
- Improve the monitoring and control of future I.S. solutions

Figure 2: Thales partner description on web site

3 Web site

The www.deserec.eu web site has been designed, developed, deployed and advertised.

It has been designed in order to show the project objectives and results as well as to collect and organise all the material related to dissemination activities.

The web site features :

- a short introduction to the project
- a collection of the recent news about the project and the web site
- a presentation-like set of introductive pages
- an overview of the different workpackages in which the project is organised
- an introduction of the project's test-beds
- a presentation of the partners involved in the project
- a description of the past and future events related to the project (like workshops)
- a section dedicated to the presentation of the dissemination activities within the project (workshops/conferences, papers/presentations, newsletter, planned activities)
- a collection of all the newsletter issues

The web site is actually composed by two main sites: a public one and a private one. The former (publicly accessible) spreads all material approved to be public while the latter serves as an internal, private web site. The private site has indeed restricted access: only internal partners can look at the contents. This has the two-fold objective of sharing internal documents among partners and of providing a way to review contents before making them public.

Figure 3: The DESEREC web site

4 Newsletter

The DESEREC Newsletter has been designed and advertised. It aims at promoting the project's results to interested users. It has multi-fold objectives :

- Inform on recent and future DESEREC activities and events,
- Summarize ongoing activities,
- Provide links to detailed material on specific subjects,
- Foster liaison with other related projects,
- Disseminate and advertise the project's results,
- Announce significant events (e.g. conferences) in the field of dependability and security.

A subscription procedure has been set up with an interface through the DESEREC web site (http://www.deserec.eu/newsletter.html).

Copies of the newsletter have been distributed during the ESFORS workshop.

4.1 Newsletter Past Issues

4.1.1 October 2006

The first issue has been released in October 2006 with the following TOC :

- Goals of the Newsletter,
- Introduction to DESEREC
- DESEREC Training workshop
- User scenarios
- Modelling requirements and system modelling
- Modelling Languages
- Policy Modelling
- Possible tools for the DESEREC solution

4.1.2 July 2007

The second newsletter has been issued in July 2007 with the following TOC:

- Goals of the Newsletter
- 1st Dissemination Workshop
- 2nd Training Workshop
- List of Recent Publications
- The DESEREC architecture
- The Design Framework
- Modelling Tools
- Formal Analysis Tools
- Simulation Tools
- Experience with DESEREC Modelling Tools

4.2 Future Issues

The third issue is planned for the first months of 2008, and the topics will possibly include : the status of the project (as it will be shown at the m18 demo and with what will be presented at the 2nd training workshop) and some end-users experience.

5 Papers and Presentations

The results of the project are submitted, as technical papers, to international scientific journals and are presented to international scientific conferences and workshops as well.

The targets of this dissemination activity are academia and research institutions as well as industry specific actors such as manufacturers, resellers and system-integrators.

5.1 Published and submitted papers

Below the published and submitted papers related to the technical and scientific activities carried out in DESEREC.

5.1.1 Published papers

1. A. Atzeni, and A. Lioy, "An estimation of attack surface to evaluate network (in)security", To appear in the *Proceedings of the 9th International Conference on Enterprise Information Systems*.

2. P. Krekora, and D. Caban, "Dependability analysis of reconfigurable information systems", in *Proc. of the 2nd Int. Conference on Dependability of Computer Systems DepCoS-RELCOMEX 2007*, pages 177-184, Szklarska Poreba (Poland), ,14-16 June 2007.

3. K. Nowak, and L. Bagrij, "Using distributed multilevel agent-based monitoring technique for automated network modelling approach", in *Proc. of the 2nd Int. Conference on Dependability of Computer Systems DepCoS-RELCOMEX 2007*, pages 61-72, Szklarska Poreba (Poland), ,14-16 June 2007.

4. P. Pérez, and B. Bruyère, "DESEREC: Dependability and Security by Enhanced Reconfigurability", European CIIP Newsletter, January/February 2007, Volume 3, Number 1.

5. M. Cheminod, I. Cibrario Bertolotti, L. Durante, R. Sisto and A. Valenzano, "Evaluating the combined effect of vulnerabilities and faults on large distributed systems", in *Proc. of the 2nd Int. Conference on Dependability of Computer Systems DepCoS-RELCOMEX 2007*, Szklarska Poreba (Poland), 14-16 June 2007.

6. M. Cheminod, I. Cibrario Bertolotti, L. Durante, R. Sisto and A. Valenzano, "Experimental comparison of automatic tools for the formal analysis of cryptographic protocols", in *Proc. of the 2nd Int. Conference on Dependability of Computer Systems DepCoS-RELCOMEX 2007*, pages 153-160, Szklarska Poreba (Poland), 14-16 June 2007.

7. D. J. Martínez-Manzano, G. López Millán, and A. F. Gómez-Skarmeta, "Multidomain Virtual Security Negotiation over the Session Initiation Protocol (SIP)", in *Proc. of the 1st International Workshop on Critical Information Infrastructures Security, CRITIS06*, Samos Island, Greece, August 2006. LNCS 4347-0249.

8. M. Sánchez, G. López, O. Cánovas, J. A. Sánchez, and A. F. Gómez-Skarmeta, "Un sistema de control de acceso para la distribución de contenidos multimedia", in *Proc. of the 9th Reunión Espanola sobre Criptología y Seguridad de la Información (RECSI '06)*, Barcelona, Spain, September 2006.

9. M. Woda, and T. Walkowiak, "Multi agent event monitoring system", in *Proc. of the 3rd International Conference on Information Technology. ICIT 2007*. Al-Zaytoonah University of Jordan, Amman, Jordan, May 9-11, 2007 / Ed. by Al-Dahoud All.

10. Ł. Bagrij, and K. Nowak, "Method for Quality of Network Services Analysis Using Queuing Modelling of Information Systems and Computer Simulation Techniques", in *Proc. of the 3rd International Conference on Information Technology. ICIT 2007*. Al-Zaytoonah University of Jordan, Amman, Jordan, May 9-11, 2007 / Ed. by Al-Dahoud All.

5.1.2 Submitted papers

W. Zamojski, R. Adamiec, T. Walkowiak "Multimedia approach to e-lectures in Flash environment", submitted to the *3rd International Conference on Information Technology ICIT 2007*

M. D. Aime, A. Atzeni, and P. C. Pomi, “AMBRA - Automated Model-Based Risk Analysis”.

D. J. Martínez, M. Gil, G. López, and A. F. Gómez-Skarmeta, “A proposal for the definition of operational plans to provide dependability and security”, submitted to the *Critical Information Infrastructure Security (CRITIS’07).*

5.2 Presentations

This section lists the workshop / conferences where presentations related to DESEREC have been done.

1. **SecurIST workshop** (22 March 2006, Brussels)
   Speaker: Benoit Bruyere (THC)
   Subject: presentation of Deserec project to other newly started European IST programs
2. **ISAS 2006 conference** (15-16 May 2006, Helsinki, Nokia Research Center)
   Speaker: Benoit Bruyere (THC)
   Subject: presentation of Deserec project as part of a session called "EU Dependability Projects Track" together with other European projects (ESFORS, HIDENETS and GST).
3. **DepCos conference** (25-27 May 2006, Szklarska Poreba, Poland)
   Speaker: Andre Cotton (THC)
   Subject: presentation of Deserec project
4. **Inauguration of the 7th Framework Programme in Poland** (16-17 November 2006, Warsaw, Poland)
   Author: Wojciech Zamojski (PWR)
   Subject: poster presentation of Deserec project at the exhibition "Polish R&D Potential"
5. **ReSIST Open Workshop** (22 March 2007, Budapest,Hungary)
   Speaker: Benoit Bruyere (THC)
   Subject: presentation of Deserec vision on managing resilience
6. **ESFORS Workshop** (10-11 July 2007, Maribor, Slovenia)
   a. Speaker: Gabriel López (UMU)
      Subject: presentation of operational plans designed in DESEREC
   b. Speaker: Antonio Lioy (POLITO) – Keynote speech
      Subject: Some thoughts for future RTD in secure software systems and services
   c. Speaker: Antonio Lioy (POLITO)
      Subject: presentation of the DESEREC project
   d. Speaker: Marco Aime (POLITO)
      Subject: Modelling services for trust and security assurance
   e. Speaker: György Csertán (BUTE)
      Subject: Model driven development of adaptive structures
   f. Speaker: György Csertán (BUTE)
      Subject: Dependability & Security Metrics
   g. Speaker: Luca Durante (IEIIT)
      Subject: Formal methods for the analysis of wide distributed systems
   h. Speaker: Luca Durante
      Subject: Engineering dynamic & ad-hoc service coalitions

5.3 Publication plan

Future publication of papers is foreseen according to the tentative schedule reported below.

5.3.1 POLITO

- A model-based methodology for risk analysis:
  how to use formal description of services and system to support a semi-automatic methodology for threats identification and risk assessment.
  Expected date: starting from June 2007

- Security metrics:
  a survey on security metrics and their applicability to system configuration evaluation.
  Expected date: starting from June 2007

- Multi-level modelling of systems for security configuration validation:
  cross-validation of service and resource models, extraction of simplified views to support specific analysis techniques.
  Expected date: starting from June 2007

- System models for system management:
  how to use DESEREC models at runtime: update system context, handle context in case of reconfigurations, ...
  Expected date: starting from November 2007

5.3.2 UMU

- Dependable and Secure Infrastructures for Communication and Information Systems:
  The aim of this work will be to show the work done in the design, definition and deployment of infrastructures for dependable systems.
  Expected date: starting from September 2007

- Enhancing dependable and secure infrastructures by means of distributed architectures:
  The aim of this work is to present how distributed architectures, based, for example, in P2P communications, can improve, the high dependability and security requirements in DESEREC.
  Expected date: starting from October 2007

5.3.3 IEIIT

- Modelling and managing the combined effect of vulnerabilities and faults in extended system
  The aim of this work will be to improve our previous work in modelling vulnerabilities and faults.
  - extended vulnerability model
  - compatibility with existing vulnerability repositories (e.g. oval)
  - enhanced representation of all the possible consequences of vulnerabilities and faults (attack graph)
  - more powerful representation of active elements (e.g. routers, firewalls ...) will be investigated
  Expected date: starting from October 2007

- Analysis of the combined effect of vulnerabilities and faults in large networks
  This work will present some results analysing a real world case study with our formal analysis tool. The aim will be to check the scalability of the tool and to verify its suitability to analyse a real world example.
  Expected date: starting from October 2007

5.3.4 ENST

- Assessment of robust overlays
  Expected date: starting from May 2007

- An architecture for resilience overlays in an ISP
  Expected date: starting from October 2007

- Improved resilience using routing overlays
  Expected date: starting from December 2007

5.3.5 BUTE

- Qualitative Fault and Error Modelling in the Model Driven Design of IT Systems
  Drawing on the general theoretical framework for qualitative fault/error/failure analysis elaborated earlier, the embeddability of the approach into a model driven system design workflow is examined. This covers
  i) the immediately applicable and the foreseen use cases introduced centered around the notion of hidden formal methods - with an emphasis on dependability consolidation,
  ii) the metamodel-based representation of existing engineering knowledge and analysis results as fault/error/failure dictionaries, component-level error propagation models and meta-level fault mechanisms and
  iii) questions of composability of said propagation models. Initial analysis approaches and results are also presented.
  Expected date: starting from July 2007

- Observation Based Validation of Meta-Level Fault Mechanisms
  In a qualitative fault/error modelling setting, fault mechanisms can be described on the meta-level in many practical cases. However, assumptions concerning the qualitative abstraction - i.e. the set of anticipated faults/errors and the mechanisms producing them - can have problems regarding granularity as well as validity in general, as they are largely based on predicted analysis needs and engineering experience. To gain trustworthy models of nonfunctional behaviour that can support off-line system analysis or on-line root cause determination, those assumptions must be validated, for example by validating the descriptions of the nonfunctional behaviour. The most general way to do this is via checking the compatibility of the observable behaviour of the actual system and the model. The elaborated approaches are demonstrated on a real-life example using a collaboration platform and its log files.
  Expected date: starting from July 2007

- Model-Based Design of Metric Driven Supervisory Systems
  The rule sets defining the behaviour of general purpose IT supervisory systems commonly employ on-the-fly computed IT metrics representing system-level nonfunctional properties to ensure dependability and security. However, metric-based high level decision making today can at the very best signal problems - the corrective action to be taken is defined using best practices. In our work, we take the first steps in introducing a model-based approach towards metrics. Most metrics have an underlying meta-level operational model - as basic finite state machines for classic dependability metrics - and a qualitative error/failure model; as a consequence, for the design of sensors and centralized supervision the Model Driven Architecture concept is directly applicable. A meta-level mechanism centric taxonomization and formalization of certain widely used metric types is given; moreover, we show that connecting qualitative fault/error/failure modelling and meta-level formulation of metric semantics opens a way for at least partially estimating the effect of reconfiguration actions on the value of the metric. We also show that how the common sense approach of sensing problems on a high level - assessing low level events prior to taking action translates to an increase of certainty in the correctness of the action to be taken in the presented cases.
  Expected date: starting from August 2007

- Economical model of spam protection
  We intend to check the current state of the art technology against spam with economical approach and to identify the possible ways to improve spam protection.

- Performance modelling of SMTP servers
  Nowadays the once simple mail servers have become a complex system: spam, virus filtering, protection against DoS, etc. The modelling and performance evaluation of these systems is not as straightforward as they used to be by defining a simple M/M/1 queue. The different types of mails and their different service time has to be taken into consideration. We plan to model such systems with novel methods from the field of performance modelling, supported by measurements from real, working systems.

- Vulnerability lifecycle modelling
  The most up-to-date articles about the lifecycle of vulnerabilities are written in around 2000. No need to mention that there has been lot of changes since then on the Internet, which could mean that these models are worn out. We plan to analyze recent vulnerabilities, compare the lifecycle of recent vulnerabilities to the earlier ones and if it is necessary define new models. The input data is from real, working environments (not only partly accessible online databases like earlier works).

- Security metrics in practice (or such)
  Defining security metrics is a difficult question. However several recommendations exist in literature. It frequently happens that the input data of these metrics is difficult to define for even a security expert. We plan to analyze and recommend such available input data which can feed with valuable information the security metrics and beside this they can be easily defined and collected.

5.3.6 PWR

- Virtual user representative - monitoring business services.
  How to monitor complex internet services (calculate some "dependability" measures, like availability) from the user side (a mimic of human user behaviour).
  Expected date: starting from November 2007

- Multilevel computer simulation approach for network services analysis.
  How to use concept of hierarchical modelling for enhancing computer networks simulations; how to define requirements regarding (multilevel) input of simulation, how to build hierarchy of model layers and how to take advantage of the idea of selective detail level.
  Expected date: starting from September 2007

- Dependability analysis of networked business services using high level simulation.
  How to define a meta-model suitable for representing several aspects of network services dependability analysis, e.g. services orchestration/choreography, usage schemas (use-cases), scenario requirements and constraints, components inoperabilities, repairs, etc.
  Expected date: starting from November 2007

- Distributed monitoring of the Complex Information Systems.
  Advantages and drawbacks, problems with firewalls, communication protocols and events formats, security.
  Expected date: starting from June 2007

- Simulation of network reconfiguration dynamics.
  Requirements of remote system management and reconfiguration. Using network simulation to identify transient inconsistencies in the configuration and vulnerabilities in the process of system reconfiguration.
  Expected date: starting from September 2007

6 Workshops and Conferences

Workshops mainly target internal end-users and present / will present some technical results achieved in the project.

Conferences are a means to spread the ideas behind the DESEREC project to a broader audience.

6.1 Conferences

The DESEREC project has been presented at the DepCos RELCOMEX 2006/2007 conference.

The information of DESEREC project (three pages) is included in the following conference proceedings:

- Proceedings of International Conference on Dependability of Computer Systems. DepCoS - RELCOMEX 2006, Szklarska Poreba, Polamd, 25-27 May 2006, Eds Wojciech Zamojski et al., Los Alamitos : IEEE Computer Society [Press], cop. 2006
- Proceedings of International Conference on Dependability of Computer Systems. DepCoS - RELCOMEX 2007, Szklarska Poreba, Poland, 14-16 June, 2007 / Eds Wojciech Zamojski et al., Los Alamitos : IEEE Computer Society [Press], cop. 2007.

And is also available from the IEEE Computer Society Digital Library at

- http://csdl2.computer.org/comp/proceedings/depcos-relcomex/2006/2565/00/2565xi.pdf
- http://csdl2.computer.org/comp/proceedings/depcos-relcomex/2007/2850/00/2850xi.pdf

6.2 Workshops

6.2.1 1st Training Workshop

The 1st DESEREC training workshop "Architecture, Modelling and Tools for increasing dependability and security of Information Systems" was held at Wroclaw University of Technology in Poland on 25-26 September, 2006.

It presented project aims, analysed test-beds and foreseen architecture. Moreover, it focused on the problem of modelling of Complex Information Systems (CIS) for dependability analysis. Additionally, presentations of some existing ICT tools for modelling, simulating and monitoring of CIS were given.

The workshop program was as follows:

- Session: **User scenarios, architecture**
  - The objectives of DESEREC project
    Thales Communications, France, Benoit Bruyere
  - User scenarios, requirements, questionnaire
    SGI, Spain, Francisco Hernández Gómez
  - Currently foreseen architecture
    IABG mbH, Germany, Maximilian List
- Session: **System modelling**
  - Modelling requirements for security/dependability evaluation and management
    Politecnico di Torino, Italy, Marco Aime
  - Introduction to modeling languages (CIM, etc...)
    University of Murcia, Spain, Antonio F. Gómez Skarmeta
  - System modelling
    Politecnico di Torino, Italy, Marco Aime

- Policy modeling
  University of Murcia, Spain, Gregorio Martínez Pérez
- Questions and discussion on system modeling

- Session: **Accompanying presentations of tools**

  - VIATRA2 model transformation framework
    BUTE, Hungary, Imre Kocsis
  - NERD
    TNO, The Netherlands, Sander Degen
  - SIMICS
    IABG mbH, Germany, Maximilian List, Karl Mayer

The workshop was a successful event with more than 50 participations: representatives of the partner institutions, prospective end-users and academia.

The presentations were recorded and the computer based training courseware was produced. It was distributed among the partners and prospective DESEREC end-users.

6.2.2 1st Dissemination Workshop

The DESEREC project has organised the 1st dissemination workshop together with the 2nd ESFORS Workshop on : "**Trust, Security and Dependability in Service Oriented Infrastructures**".

Detailed program:

- Future R&D in Secure Software Systems and Services : Gap Analysis
  - Welcome by Organisers and EC
  - "Security, dependability and Trust in ICT-FP7 : Coming Issues", speech by Dr. Thomas Skordas (Deputy Head of Unit INFSO-F5 "Security", EC)
  - 2 keynote speakers :
    - Prof. Antonio Lioy (Politecnico of Torino, Italy) "Some thoughts for future RTD in secure software systems and services"
    - Prof. Miroslaw Malek (Institute of Information, Humboldt-University of Berlin) "The Power of Prediction for Adaptive, Dependable Service-oriented Computing"
  - Report on conclusions of previous Paris Workshop
  - FP6 Project Presentations : DESEREC, SERENITY, Resist
  - Engineering dynamic & ad-hoc service coalitions: design and operational (run-time) TSD aspects
    - Chair : Dr. Luca Durante (IEIIT-CNR Italy)
    - Rapporteur : Jean Christophe Pazzaglia (SAP Research Center, France)
  - Scalable and adaptive ubiquitous service infrastructures
    - Chair : Dr. Antonio Maña (University of Malaga, Spain)
    - Rapporteur : Aljosa Pasic (Atos Origin, Spain)
  - Alignment of security and trustworthy services: Interoperable security policies, business, socio-economic and legal aspects
    - Chair: Reijo Savola (VTT Technical Research Centre of Finland)
    - Rapporteur: Prof. Bernhard M. Hammerli (ACRIS, Switzerland)
- Resilience in Services and Service Infrastructures
  - 2 keynote speakers :

- Prof. Paulo Verissimo (University of Lisbon, Portugal) "Resilience Challenges in Service-Oriented Architectures"
- Dr. Gregory Chockler (IBM Haifa Research Laboratory) "Towards a Peer-to-Peer Middleware Platform for Highly Scalable and Robust Service-Oriented Computing"

- Resilience in service oriented infrastructures
  - Chair : Dr. Edgar Weippl (Secure Business Austria)
  - Rapporteur : Pedro Carvalho (University of Lisbon, Portugal)
- Resilience in Software Systems and Services
  - Chair: Prof. Peter Ryan (Newcastle University, UK)
  - Rapporteur: Sandy Johnston (Hewlett-Packard, UK)
- Resilience in Business Processes
  - Chair : Luca Save (DeepBlue, Italy)
  - Rapporteur : Domenico Presenza (Engineering, Italy)

Refer to WP5 deliverables for further details on this event.

6.3 Planned activities

In addition to regular publications as previously described, some exceptional events are planned in the next period for communicating on project concepts and achievements.

6.3.1 2nd Training Workshop

In September 2007 the DESEREC project will host the second training workshop: "**The Mechanisms used for Increasing Dependability through Enhanced Reconfiguration"**, in Athens, Greece.

The 2nd Training Workshop addresses vital topics of system security and dependability and engineered mechanisms for enhancing them. Organisation of the event is performed by ICOM partner. The DESEREC web site provides advertising of the event with leaflet and access to registration form hosted by ICOM web site.

Target audience includes but not limited to:

- Software engineers
- System security managers/administrators
- Business service managers

As people external to the DESEREC project will attend this event, it will also be a dissemination workshop.

Refer to WP6 deliverables for further details on this event.

6.3.2 2nd Dissemination Workshop

The planning and organization of the 2nd Dissemination Workshop (possibly jointly with the workshop on "Case studies of Increasing Dependability") will start in the second period of the project.

We plan to combine it with the 3rd training workshop "The Results and Applications of DESEREC" planned at M33.

6.3.3 3rd Training Workshop

At M33, a third training workshop is planned called “The Results and Applications of DESEREC”

Target audience includes but not limited to:

- Software engineers
- System security managers/administrators
- Business service managers

Refer to WP6 deliverables for further details on this event.

7 Exploitation Plan

As part of such European research projects, the exploitation of DESEREC results is one the main objectives of industrial partners as well as end-user partners. Each industrial and end-user has elaborated its plan for exploitation as introduced in the Description of Work. These exploitation activities will be further refined as the project progresses. Here below is the initial exploitation plan.

THC delivers and supports customers mission-critical information systems. Most of the organisations need to interact with others, each day with shorter delay to improve the supply chain performance.

The overall interest of THC in DESEREC is to improve the dependability of its systems, and more especially its systems of systems. The project will help THC to enhance the hot and fast reaction mechanisms, and the high-level decision processes, to guarantee to its customers a high level of resilience and to provide tools to operate reconfiguration operations.

EADS is a provider of secure communication network for public safety operation requesting strong security and resilience. EADS will develop, assess and validate the solutions to improve overall system dependability that are designed by DESEREC.

This project will be very useful for **EADS** to develop new algorithms to ensure management and resilience of complex and large system composed of heterogeneous devices. Indeed system management solution with efficient means to control, monitor and react constitutes a keystone for EADS future large system for enhancing their dependability while increasing their complexity and decreasing their maintenance and exploitation costs. After this project, these new management technologies would be packaged in order to offer to EADS DCS clients global turnkey system with powerful management means allowing to react in less than a day dimension to a wide range of incidents.

IABG has two main interests for exploiting DESEREC results:

1) IABG is running its own Teleport at IABG, providing Internet connectivity via satellite. As an own Teleport operator must of course take care about the operational security issues of the system and service. Detecting incidents and addressing them in the right way is a key here.

2) IABG support many key customers, such as the car manufacturer or the governmental institutions, concerning security issues of their networks. This support could be only consultancy work, but could also be verifying the security of an outsourced network or prototyping and testing new security components. Again here the detection of incidents as well as the way to address them are important aspects.

GMV/SGI is a major Spanish provider of logical security solutions. As such, SGI is very interested in assessing and testing the potential techniques and technologies that are able to improve system dependability. The results from DESEREC project may give input to SGI's solution development process, leading to enhancements of the company's portfolio. SGI is especially interested in developing new aggregation and correlation algorithms that help to tackle the "false-positive problem", thus reducing the amount of security event information that must be checked manually.

SGI expects that the DESEREC project helps to understand the problem. Based on a positive proof of these new algorithms in trials, SGI will position its solutions into its marketing, product management and product development plan.

OTE, being the leading telecom operator in Greece and the Balkan area, is already heavily involved in the area of security. OTE is the former incumbent operator in Greece, and as such, owns and operates most of the critical telecom infrastructure installed in the country. Further OTE owns various companies in the Balkan are (such as the former incumbent of Romania, Armenia, etc).

Therefore securing its telecom infrastructure is very critical, and already many security mechanisms and procedures are being used. However, recent developments in the area of security indicate that a more comprehensive and systematic approach is needed. Current mechanisms and procedures provide

adhoc security but OTE lacks an integrated security mechanism, tailored for its needs. The recent experience from the Athens 2004 Olympic Games with their stringent requirements showed that such a system would greatly simplify and improve security, and at the same time it would reduce the security operating costs. Therefore OTE is interested in the exploitation of the DESEREC project results, and plans to introduce them in its infrastructure.

TL offers both products and services in the area of embedded software with high security requirements. The company already has strong positions in the smart card and cellular phones market and intends to exploit the results of the DESEREC project to extend its offer to cover secure software for network nodes (routers, policy decision points, gateways, etc.). Security requirements are growing for such components and this area can benefit from the experience of TL in traditional security critical areas such as banking, access control or identification. To this aim, Trusted Logic further develops its offer in terms of secure components (especially based on its "Security Module" which is Trusted Logic core software component for embedded systems) and extend it to take into account the specific needs of dependable network infrastructures (secure event monitoring, management of intrusion data basis, reconfiguration and management of a survival state, etc.). More precisely, TL will:

- Use the specific security requirements and architecture put forward in DESEREC to support a dedicated version of its Security Module for dependable network nodes (routers, gateways, etc.).
- Build on the expertise gained in the security requirements for dependable networks within the project to extend its security services market (security analyses, security evaluations, help in the preparation of documents for Common Criteria certifications) in the area of dependable networks.

As part of its Integrated Platform Management solutions portfolio **ICOM** has invested on the Content Delivery Network (CDN) platform that appeared as a product in early 2005. CDN enables the delivery of services such as Digital TV (live broadcasted channels), Pay-per-View and NVoD (movies and special events), VoD and AoD, Digital Music (live radio channels), Integrated Telephony Services and applications (advanced telephony applications on TV and IP-telephony management), Walled Garden Web Portal (Data services on TV and PCs), T-commerce and TBetting Applications, Information Services on multiple client devices, and Targeted Advertisement.

ICOM plans to exploit the results of DESEREC by appropriately applying them to the CDN platform. The expertise that is acquired in the course of the project will be used so as to increase the level of dependability and strengthen the resilience of CDN to threats to the extent possible. Issues that fall in the scope of DESEREC and are expected to enhance the security and dependability capabilities of CDN include assessing and depicting the threat variants of the system through modelling, deploying a holistic threat detection schema, accumulating past knowledge and adapting to the current situation so as to comprehend and identify undesired behaviour in any given context, and having the system reconfigure itself to deter undesired modes of operation.

EXAPR is a French editor of security information management software. Since 2001, the company has been editing and marketing the software suite EAS™ (ExaProtect Advanced Software) specialized in the consolidation, correlation, treatment and archiving of security events. EAS is a SIM/ESM product (Security Information Management/Enterprise security Management) providing real time correlation of all security events and aiming at controlling the company's Information System global security. It offers synthetic and quick visibility of the alerts in progress as well as of incorrectly parameterized systems. The correlation engine is based on Exaprotect's "incident Care" technology®. It optimizes the treatment of events and provides operational, organizational and strategic security dashboards. In terms of risk management, the product enables organizations to become and remain compliant with legal requirements related to customer data protection (ex: GLBA, HIPAA, Sarbanes-Oxley, BS-17799...)

EXAPR's research activity has many common aims with WP 3 and 4 and intends to exploit the results on four main points:

1. To extend the possibility of the correlation engine included in the EAS solution (ie: modelization of complex scenarios)

2. To add to the EAS solution the capacity to automatically propose a reaction plan to security analysts (improve assistance mechanism for better human reaction)

3. To improve the knowledge and expertise of the R&D team on modelization of attacks and critical situations

4. To benefit from the lead in event modelling and complex event processing

The next generation of the Incident Care technology will include the results of the DESEREC project.

End of document.