CCLRC
Rutherford Appleton Laboratory

CORAS
http://coras.sourceforge.net

Security Risk Assessment for Web Applications

Theo Dimitrakos

Business and Information Technology Department
Central Laboratory of the Research Councils
Rutherford Appleton Laboratory, UK

CCLRC Rutherford Appleton Laboratory

Structure of presentation

- summarise some of the main contributions of CORAS
- provide an example
- ideas for future collaborations
- Other activities of interest in information security
- open discussion -- your feedback & contributions

CCLRC Rutherford Appleton Laboratory

Main contributions

- ☑ Model-based Risk Analysis
- ☑ The CORAS Framework
- ☑ The CORAS Platform
- ☑ The CORAS trials

Motivation

Qualitative methodologies for analysing risk lack the ability to account for the dependencies between events, but are effective in identifying potential hazards and failures in trust within the system, whereas tree-based techniques take into consideration the dependencies between each event.

1. combini… …t complementary risk assessment methodologies with

All aspects of dependability should be considered together as a coherent whole.
A coherent analysis of all aspects of dependability is by far more effective than the sum of the analyses of each aspect in isolation.

2. a…

The complexity of today's IT dependent systems increases the complexity of the risk of analysis tasks and demands for the co-use and/or integration various tools providing clear and easy-to explore view of the system at hand, as well as, tools supporting specific risk analysis methods and tasks

3. I…

The CORAS consortium

Facilitating collaborations with ongoing or future European R&D projects

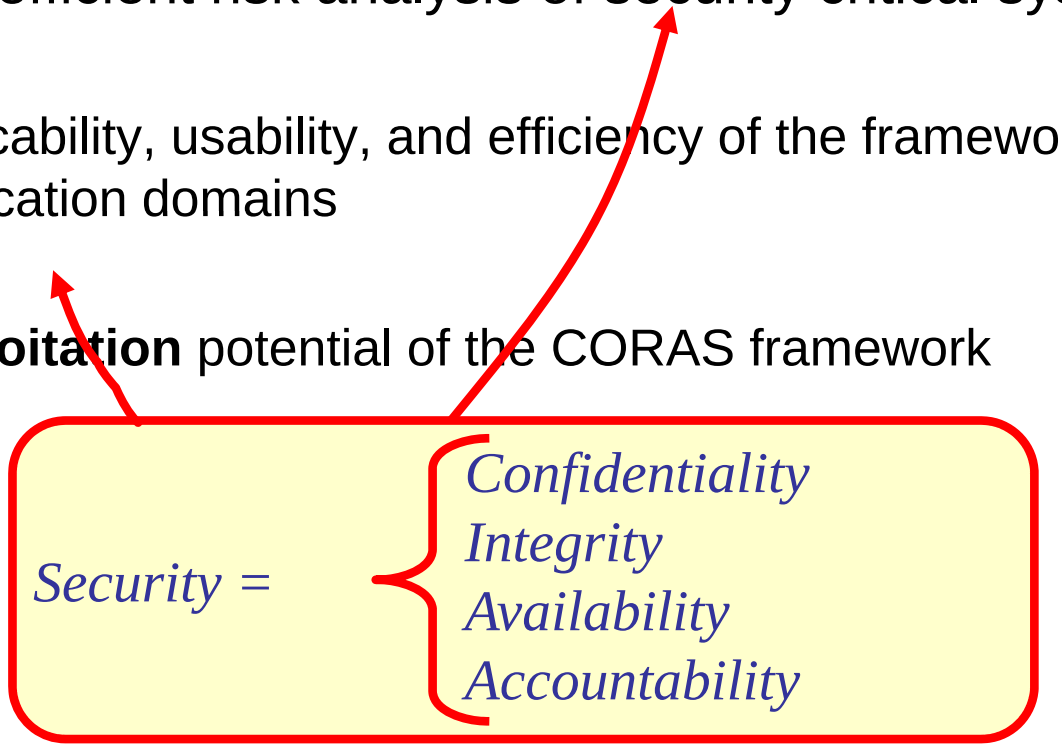
Facilitating post-implementation activities and industrial take-up

CLRC Rutherford Appleton Lab.	**[UK]**	**R&D**	*Architecture - Data-oriented Tool Inclusion - Clustering WP leader*
Computer Technology Institute	**[Gr]**	**IT Academic**	
Institute for Energy Technology	**[No]**	**R&D**	
INTRACOM	**[Gr]**	**Commercial**	*eCommerce Trials*
National Centre for Telemedicine	**[No]**	**Medical**	*Telemdicine Trials*
School of Medicine, Univ, of Crete (subcontractor)	**[Gr]**	**Medical**	
Norwegian Computing Centre	**[No]**	**R&D**	
University of London (QMW)	**[UK]**	**IT Academic**	*Scientific Coordinator*
SINTEF	**[No]**	**R&D**	*Administrative Coordinator*
SOLINET	**[DE]**	**Commercial**	
TELENOR	**[No]**	**Commercial**	
FORTH	**[Gr]**	**R&D**	

The CORAS objectives

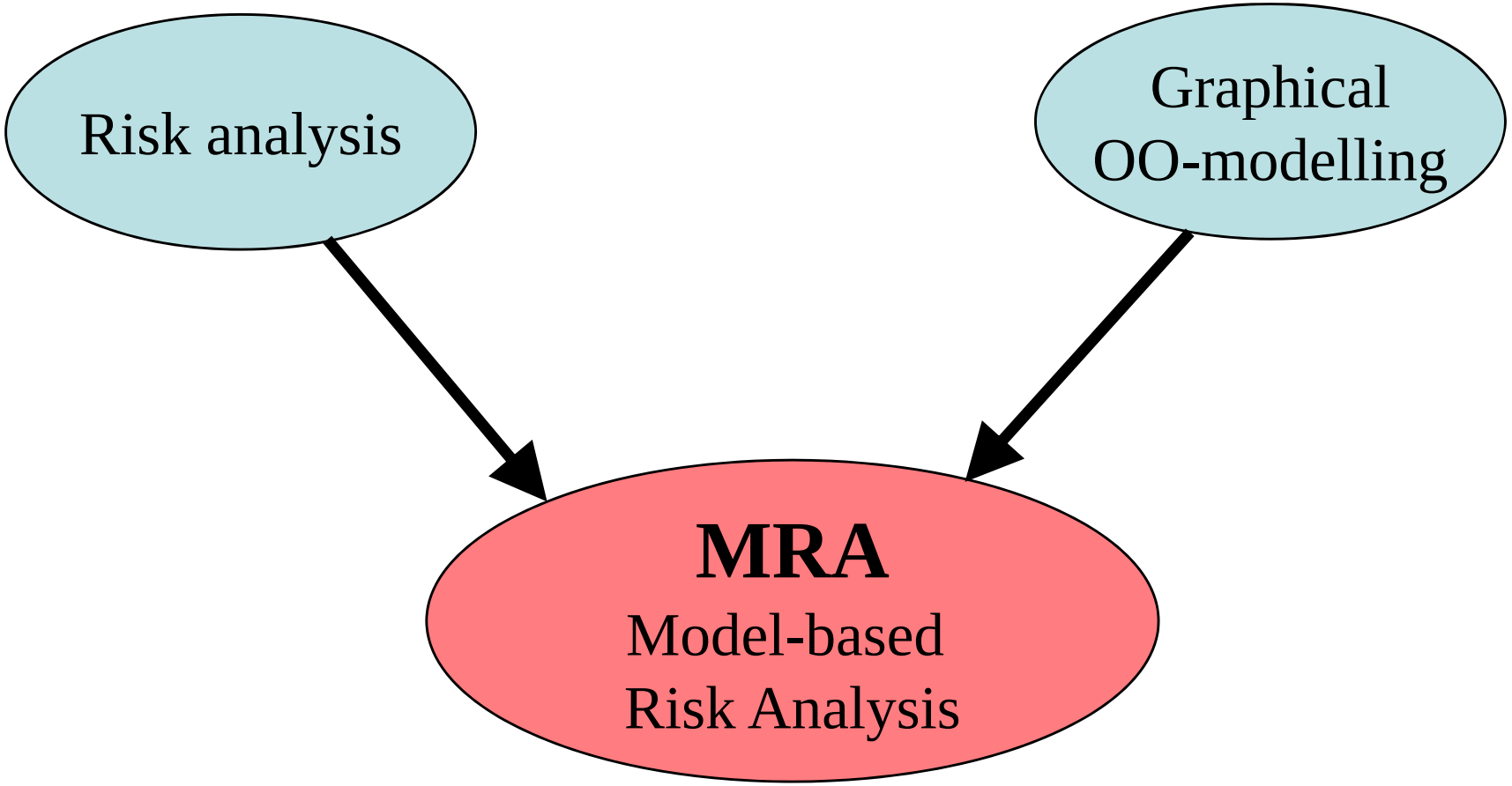
- To **develop a practical framework**, exploiting methods for
  - risk analysis,
  - semiformal object-oriented modelling, and
  - computerised tools,

  for a precise and efficient risk analysis of security critical systems
- To **assess** the applicability, usability, and efficiency of the framework by applying it in security critical application domains
- To promote the **exploitation** potential of the CORAS framework



The CORAS approach:

Model-based Risk Analysis (MRA)



Model-based Risk Analysis

Why use it?

The model-based approach **improves the quality and effectiveness** of the risk assessment process by facilitating precision, communication and interaction between stakeholders and **reduces maintenance costs** by increasing the possibilities for reuse

What does it offer?

The model-based approach provides a **semantically rich, uniform**, **streamlined approach** for each stage in a risk assessment project, from **context identification**, through **risk assessment, analysis and treatment** to **presentation of the results**

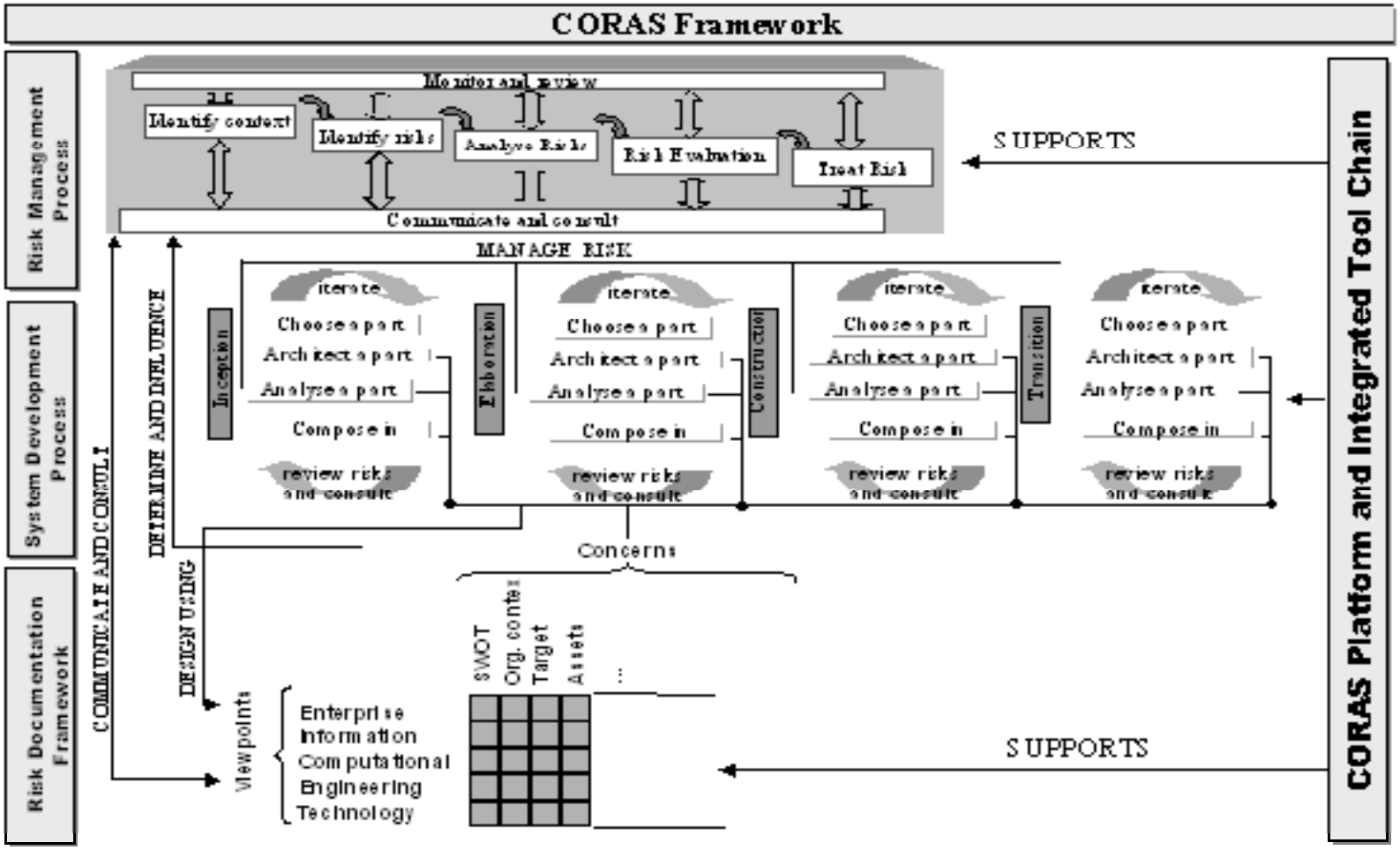
CCLRC Rutherford Appleton Laboratory

The CORAS Framework

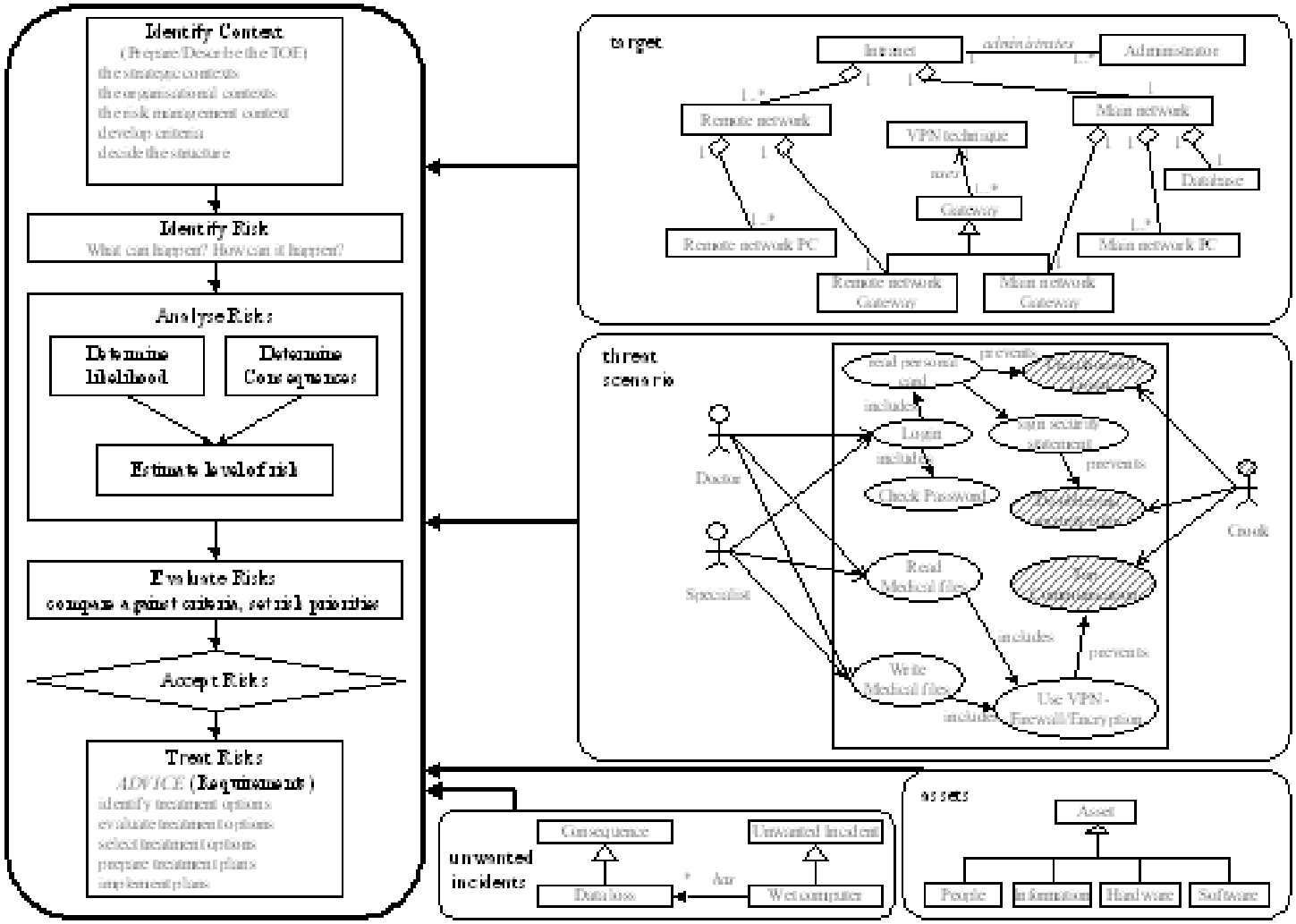
- ☑ A model-based risk assessment methodology combining
  - features from partly complementary risk assessment methods (e.g. HazOp, FTA, FMECA, Markov, etc.) as well as
- ☑ A risk documentation framework based on an extension of the ISO standard RM-ODP (Reference Model for Open Distributed Processing) with Risk Analysis
- ☑ A risk management process based on the international security risk management standards AS/NZS 4360 and ISO/IEC 17799.
- ☑ An integrated risk management and systems development process based on the UP (Unified Process) for information systems development, and integrating several complementary widely applicable risk assessment
- ☑ A platform for tool-inclusion based on XML (eXtensible Markup Language) technology allowing the integration of tools from both the risk analysis and the information systems modelling domains.

CORAS process:

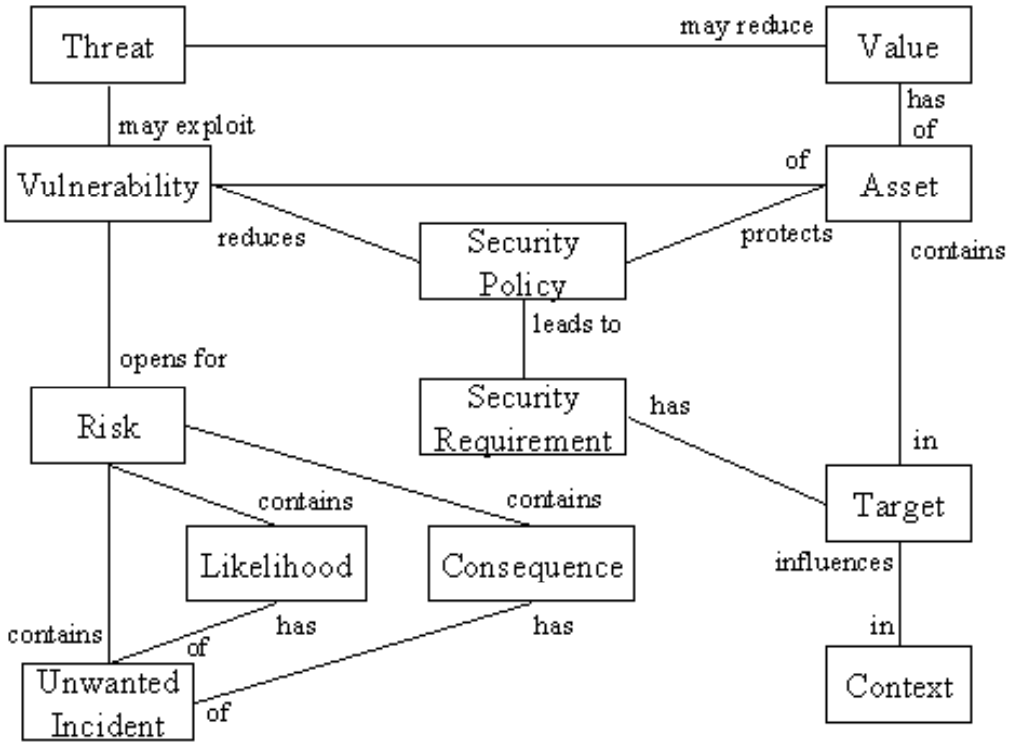
integrating Security Risk Management and the (Rational) Unified Process



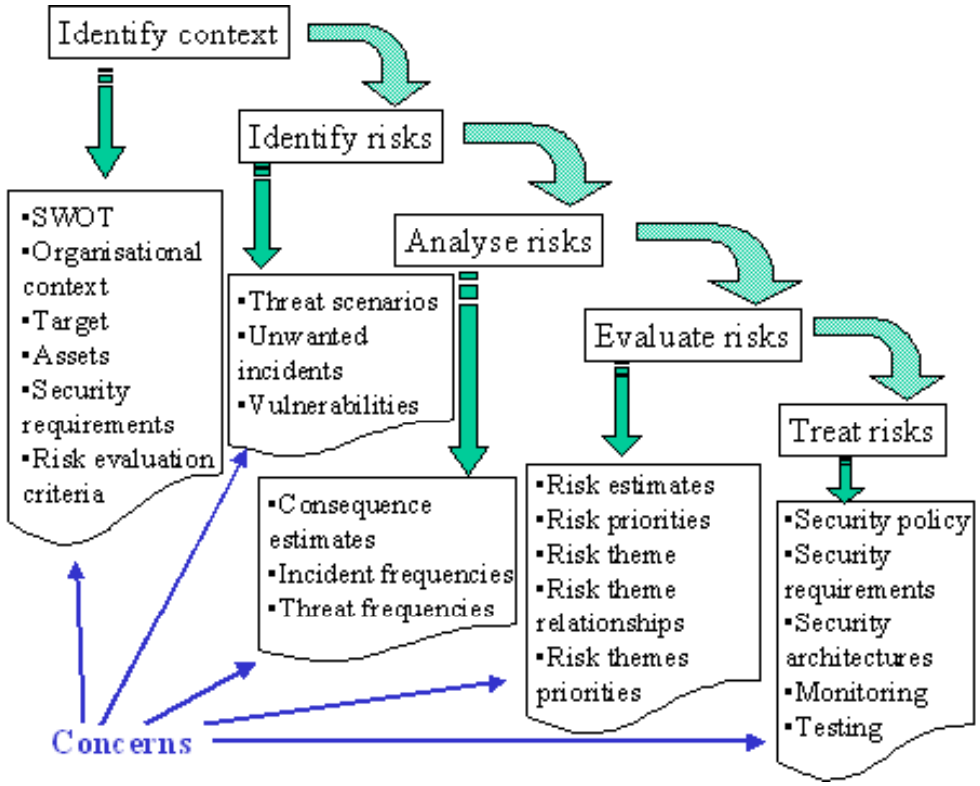
Modelling support for RA



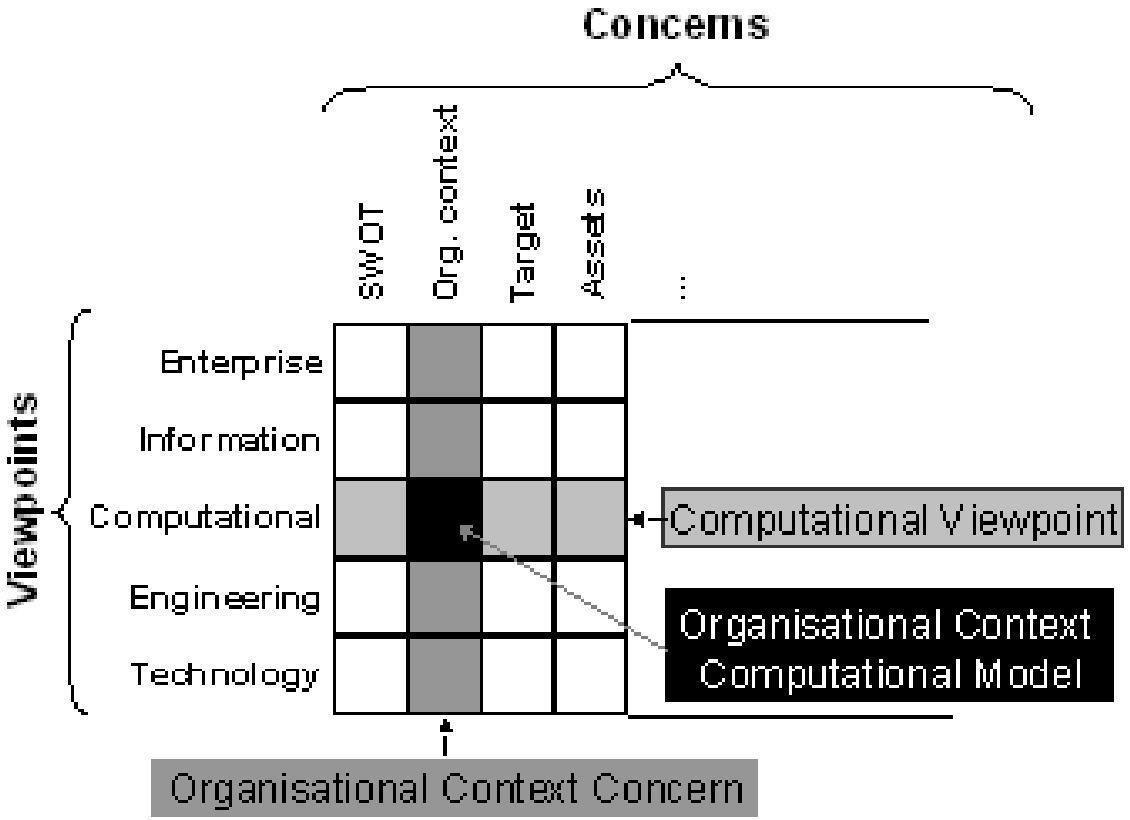
Understanding RA concepts



Introducing RA Concerns related to Risk Management Workflow



Risk Assessment Concerns as modelling concepts extending RM-ODP



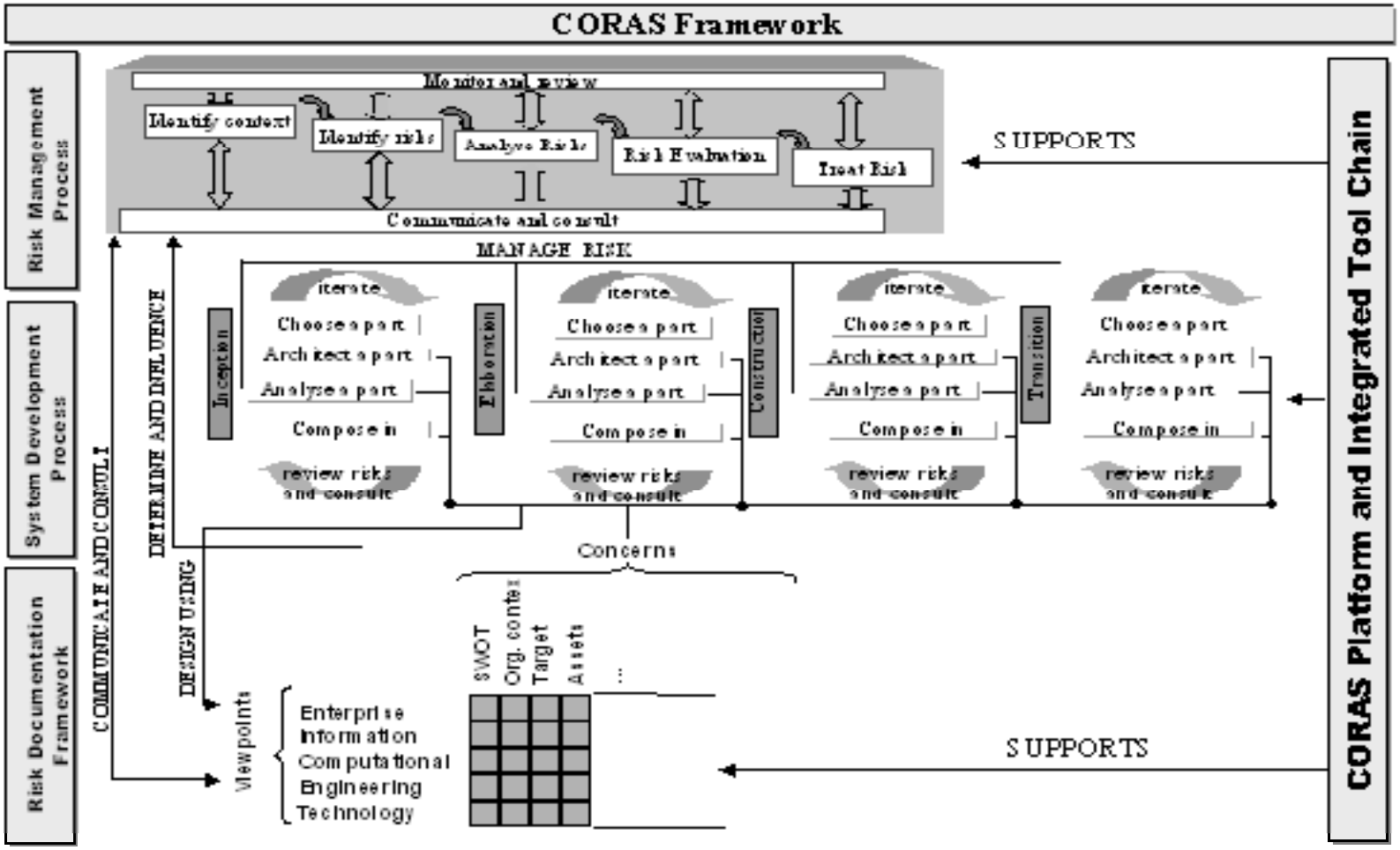
CCLRC Rutherford Appleton Laboratory

Example of dependencies between RA techniques

To → ↓From	HazOp	FTA	FMECA
HazOp	HazOp identifies incidents at different levels of abstraction.	The incidents identified by HazOp are inserted in fault trees based on abstraction level and the relationship between the incidents.	Incidents identified by HazOp may be understood as failure modes and thereby can be considered as starting points for FMECA.
FTA	A basic event (a leaf node in the fault tree representing an incident) may correspond to a sub-system/service on which HazOp may be applied.	A fault tree may be part of another fault tree, i.e., the top incident of one fault tree may be a causing incident in another fault tree.	Basic events (leaf nodes in the fault tree representing incidents) may be understood as failure modes and thereby can be considered as starting points for FMECA.
FMECA	From a basic incident (failure mode) one can associate a sub-system/service for applying HazOp on.	The analysis of a basic incident (failure mode) may identify a scenario leading to an unwanted incident. This may be represented as a path in the fault tree.	Basic incidents (or failure modes) may lead to incidents that are basic incidents (failure modes) in another FMECA.

CORAS process:

integrating Security Risk Management and the (Rational) Unified Process



Model based Risk Assessment

Tool inclusion platforms

- It is more cost-efficient to integrate specialised tools (which have been developed and test over decades and people are familiar with) rather than re-invent tool support in the context of an integrated methodology.
  - A plethora of system design, modelling and system analysis tools,
  - A significant number of specialised risk assessment tools

- A tightly integrated tool-chain is not necessary the best solution
  - Different enterprises have often their own legacy systems for design and/or risk assessment while the design and risk assessment tool specifications often change without preserving backwards compatibility.

- A “loose” tool inclusion platform
  - based on standardised representations of modelling and risk assessment meta-data
  - allow users to plug-in their preferred tools using commonly agreed or standardised and extensible exchange formats.

Tool inclusion platform

The CORAS tool inclusion platform is being built around internal data representations expressed in XML and is realised by means of three interfaces for XML based data exchange:

- An interface based on IDMEF and developed by the Intrusion Detection Working Group. (Intrusion Detection Exchange Format).
- An Interface based on XMI (XML Metadata Interchange) which is an exchange format for UML modelling tools standardised by the Object Management Group.
- An interface targeting risk assessment tools which (in the absence of any exchange format standard) is based on a proprietary meta-data presentation of the core data elements of a large number of security and safety risk analysis methods.

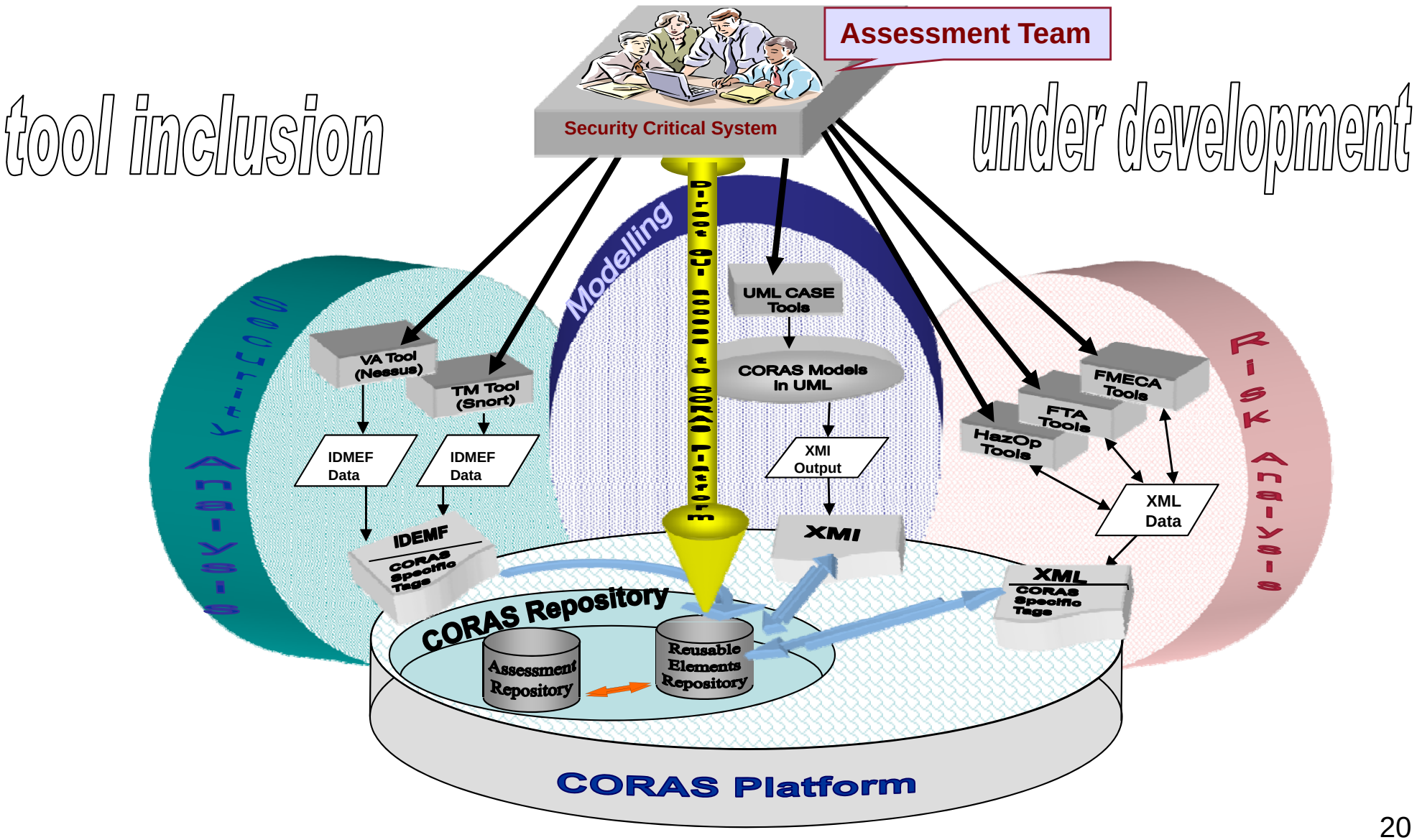
Tool inclusion platform

(1) An assessment repository storing the concrete results from already completed assessments and assessments in progress.

(2) A reusable modelling elements repository storing reusable models, patterns and templates from predefined or already completed risk assessments.

The implementation of the deployment model depicted in the following slide under continuing support and further development.

The CORAS Framework



The CORAS trials

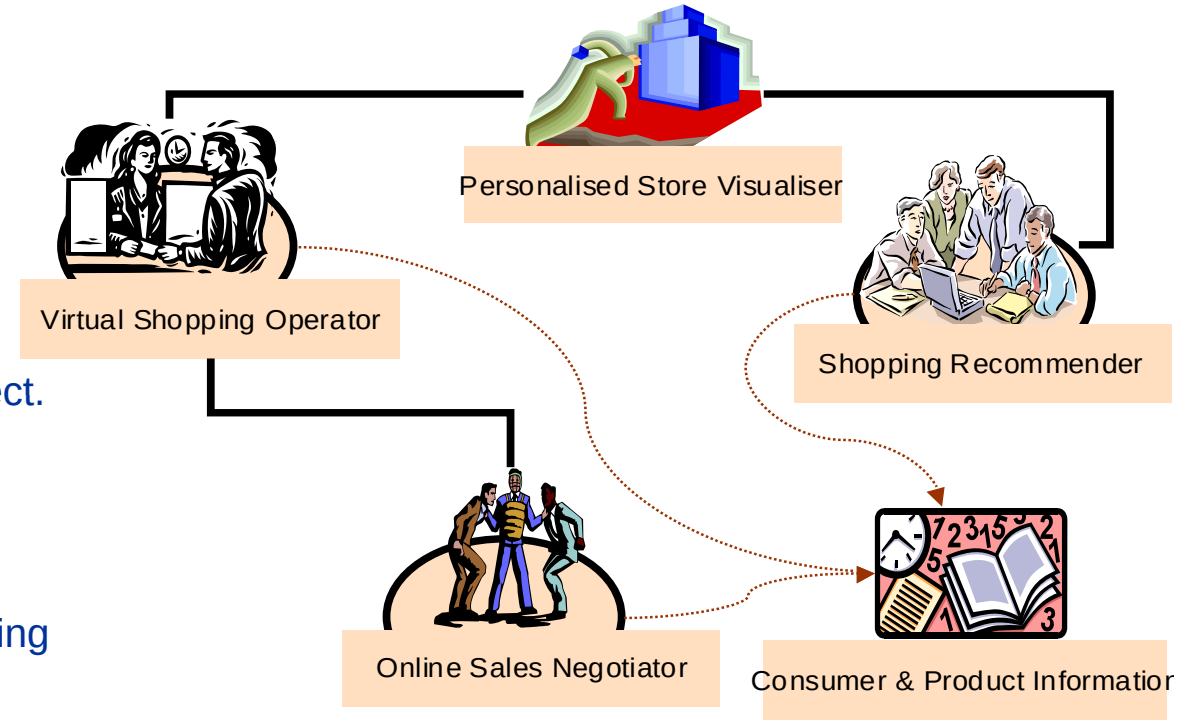
CORAS in E-Commerce

CORAS is being applied to the electronic retail market subsystem of an e-commerce platform, developed in another European Union IST project.

The security assessments focus on

- the user authentication mechanism,
- the secure payment mechanism and
- the use of software agents for accomplishing specialised purchasing tasks,

offering a process for identifying and assessing potential solutions



The CORAS trials

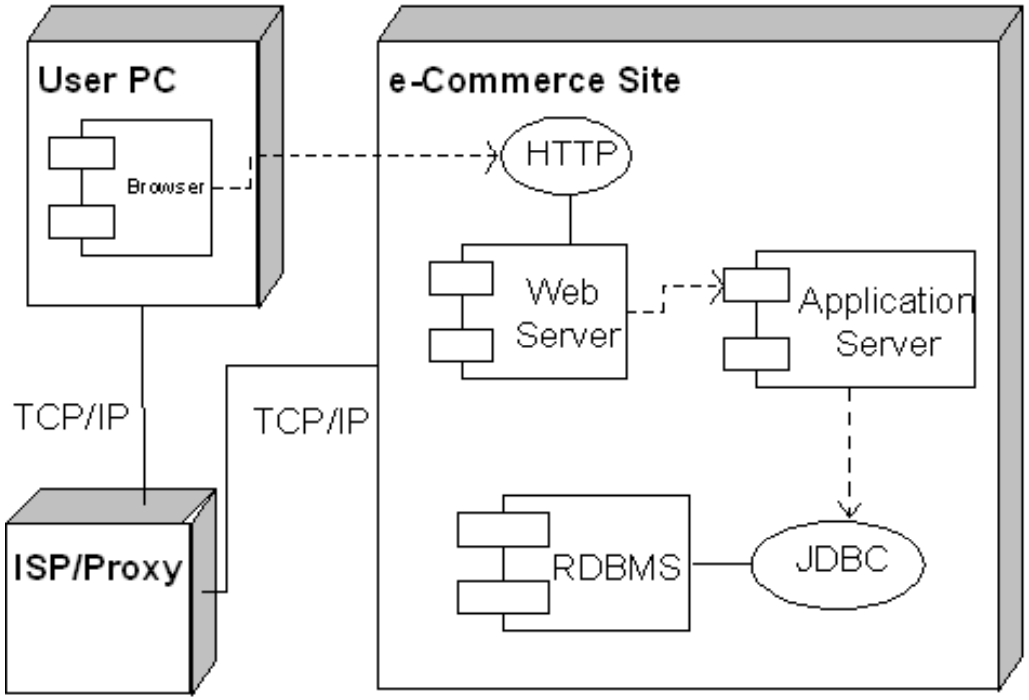
CORAS in Telemedicine

CORAS is being applied to the regional health network **HYGEIAnet** that links hospitals and public health centres in Crete

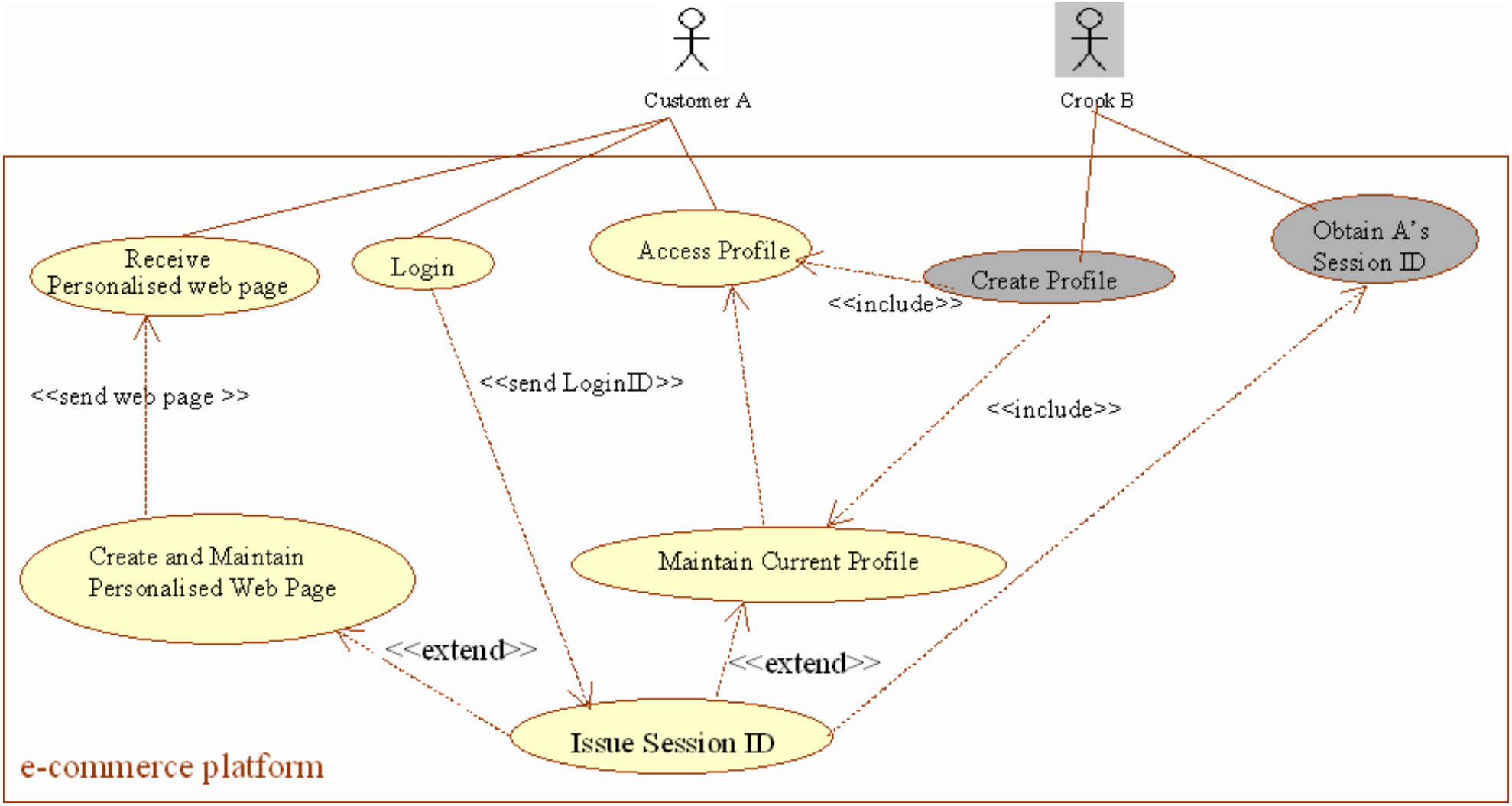
CORAS provides the security assessment of the Cretan health care structure that consists of a number of geographically separated health care centres in a hierarchical organisation

CORAS offers a process of identification and assessment of potential solutions

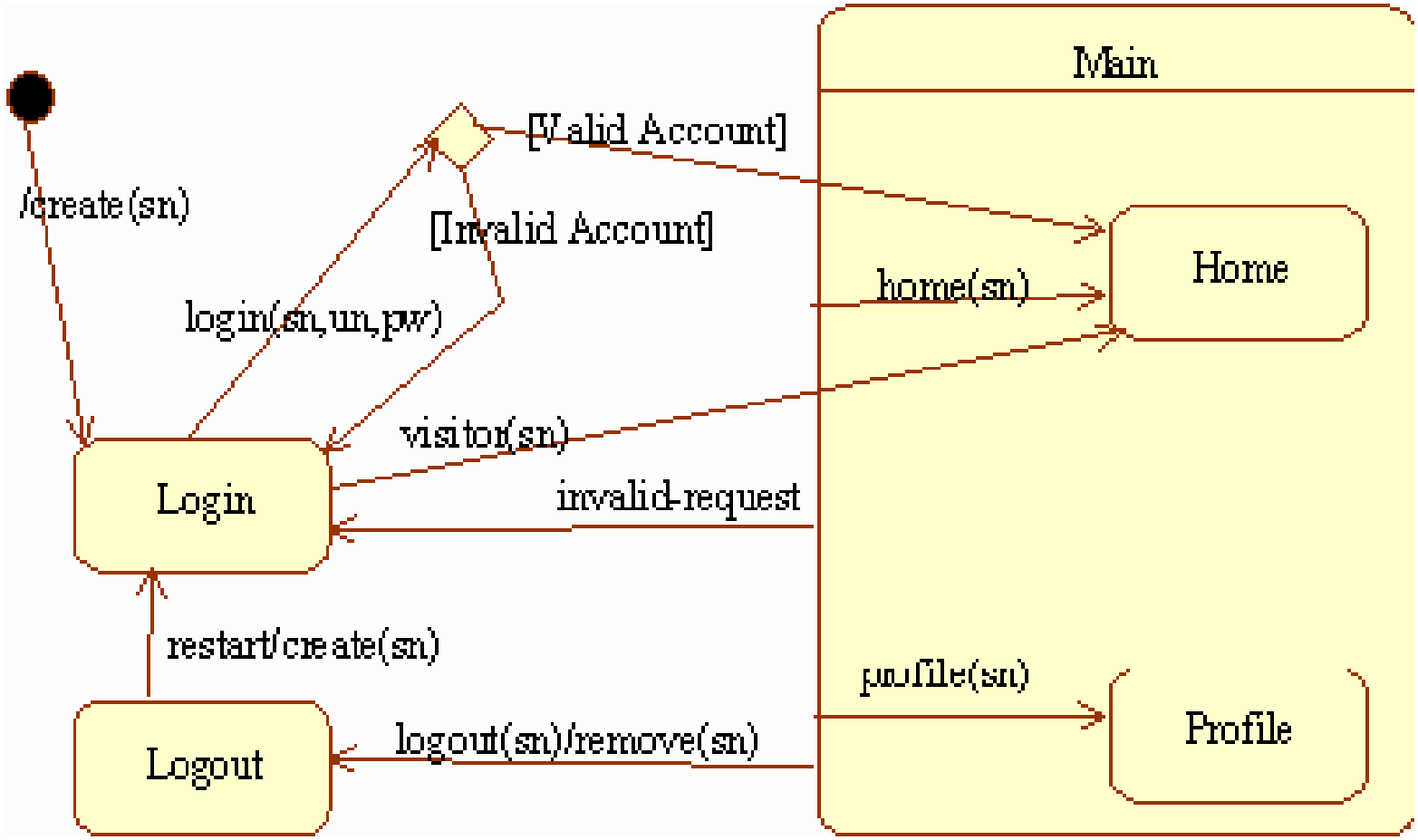
Example: *part of e-commerce trial*



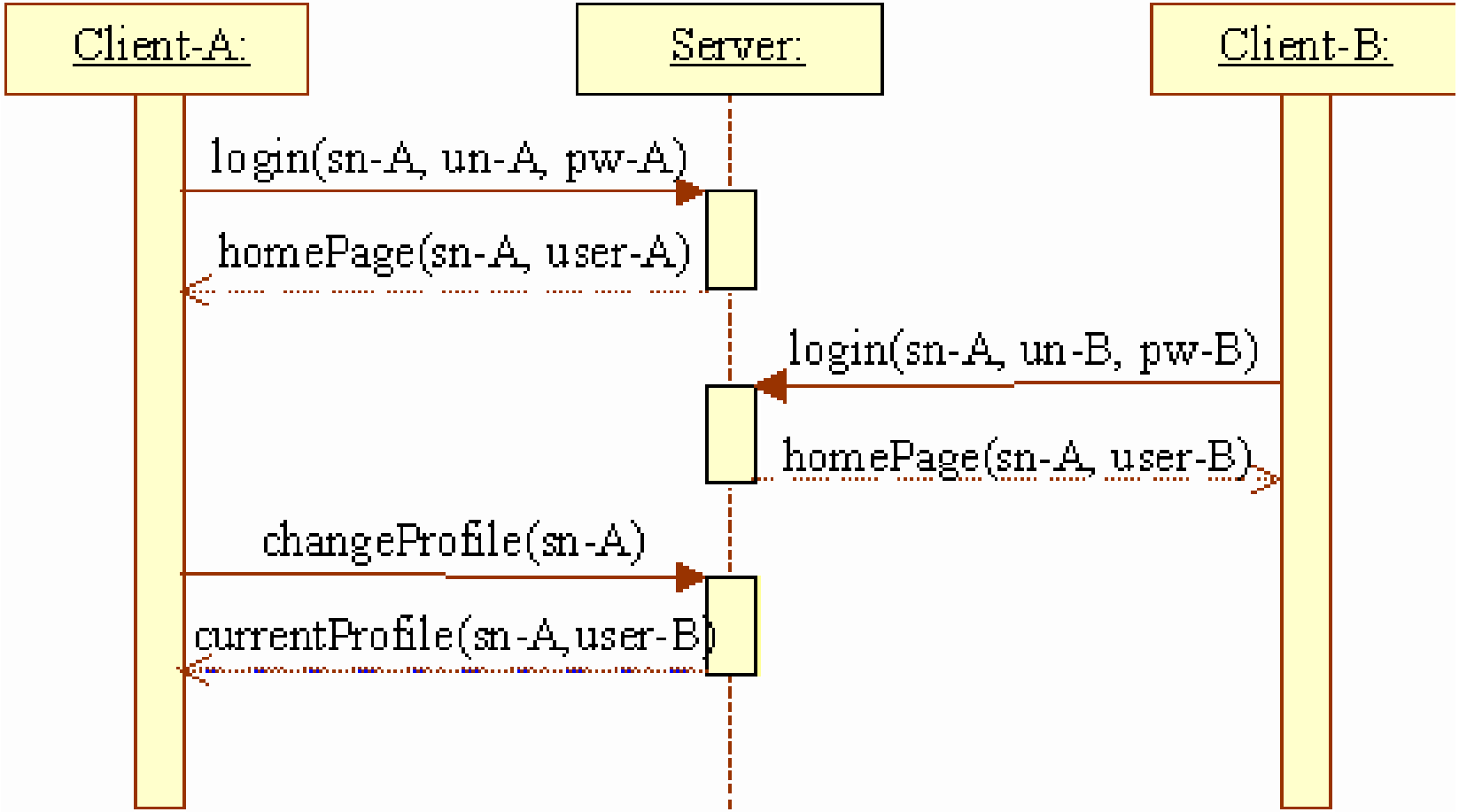
Example: *part of e-commerce trial*



Example: *part of e-commerce trial*



Example: *part of e-commerce trial*

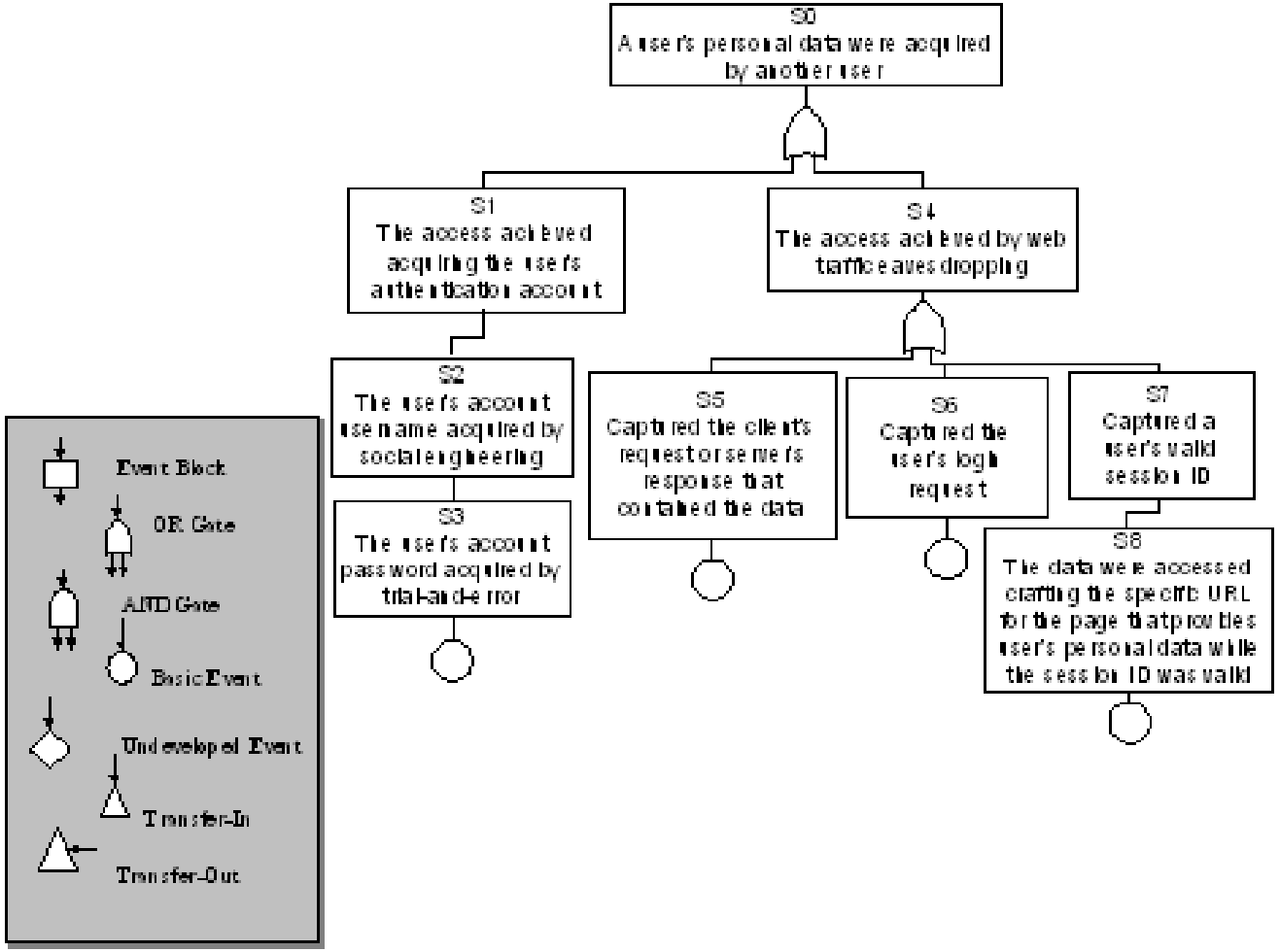


CCLRC Rutherford Appleton Laboratory

Example: *part of e-commerce trial*

No.	Entity	Description	Security attribute	Deviation	Causes	Consequences	Actions	Remarks
1	^create (sn)	A user requests to access the Login Page. Server creates a new session number (SN)						
1.1			Disclosure					
1.1.1				User request captured	Openess of Internet	Not exploitable	N/A	No confidential information transmitted
1.1.2				Server response captured	Openness of Internet	SN revealed to capturer	No encryption justified	Deliberate session hijacking is possible
1.2			Manipulation					
1.2.1				A browser or proxy responds with a cached page	Browser or proxy (mis)configuration	User gets a page with invalid SN	N/A	The Login page will returned in the following client request
1.2.2						User gets a SN used by another user	Use large numbers for SN	Inadvertent session hijacking
1.3			Denial / Delay					
1.3.1				User request is blocked by proxy server	Proxy configuration	Server is not accessed	N/A	The server is not accessed
1.3.2				Server response is too slow				Generic deviation
1.4			Unaccountability					
1.4.1				Artificially large number of requests are generated	Deliberate server attack	(1) Creation of too many SNs (2) Server performance degradation	Block access based on client's IP address	Sensitive issue for SN-based user identification

Example: *part of e-commerce trial*



Working with others …

CORAS has been one of the few IST projects that have put aside resources for actively pursuing collaborations with other European R&D projects.

Goals of CORAS "Clustering" Workpackage:

To establish close collaborations with selected projects and actors, within the following communities

- **eHealth,**
- **eCommerce,**
- **Dependability,**
- **Trust & Security**

Collaboration with other ongoing projects included

- use of **CORAS** framework by other projects,
- use of other projects' results for case studies within **CORAS**,
- joint trials or demonstrations if feasible,
- joint events

Working together …

CCLRC and SINTEF are actively seeking opportunities for cooperation towards continuing the development of the CORAS approach.

Technical cooperation may target at the further development or commercialisation of the CORAS tools and methods.

Government and businesses may take advantage of the CORAS technology in order to improve their mission critical risk assessment while evaluating the CORAS approach.

contacts:

Theo.Dimitrakos@rl.ac.uk CCLRC-RAL

Ketil.Stoelen@sintef.no SINTEF

Other activities of interest

FP5 Project

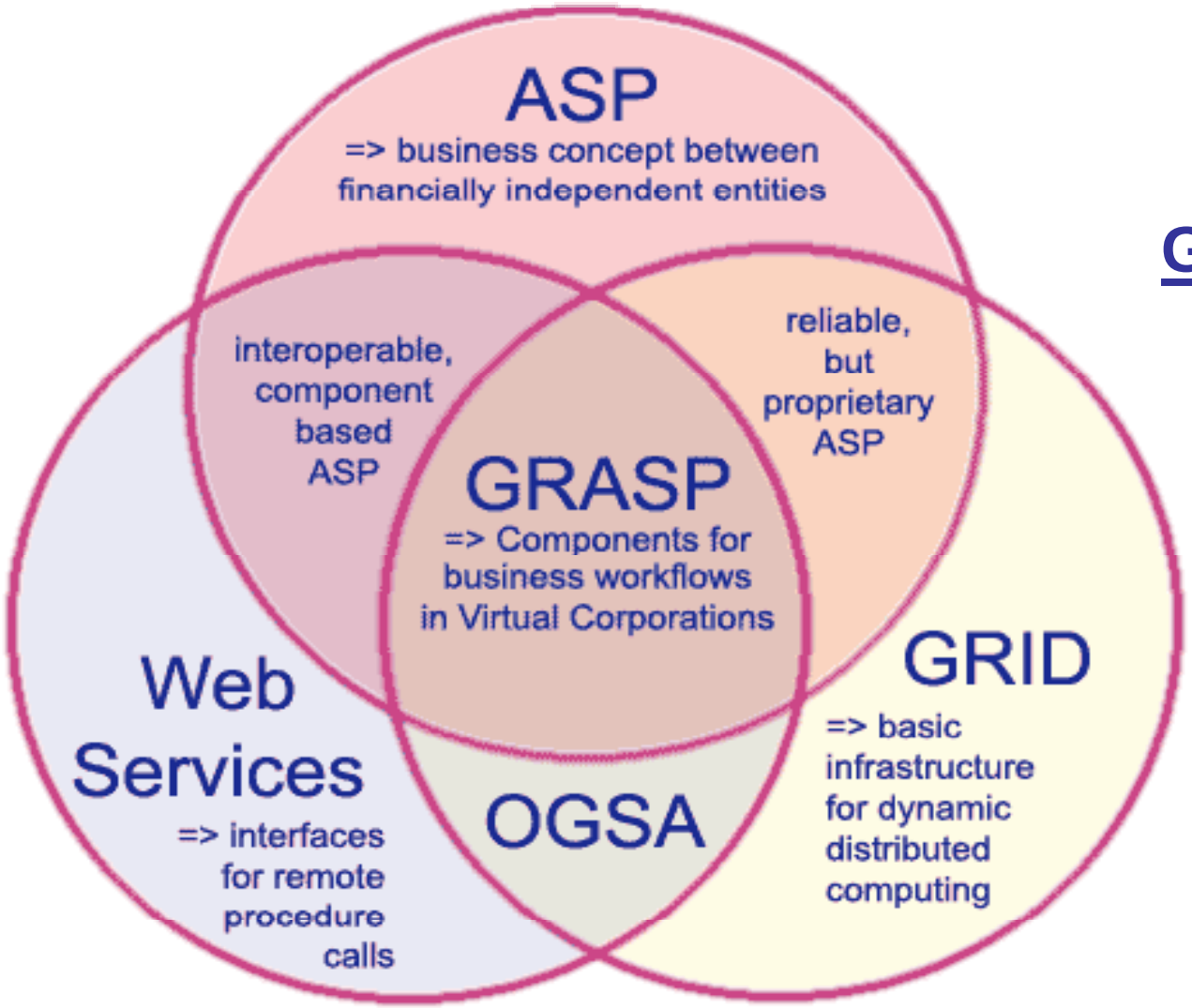
04/2002- 12/2004

Presenter: Theo Dimitrakos
Affiliation: ISE Group, BITD

CCLRC Rutherford Appleton Laboratory

GRASP integrates

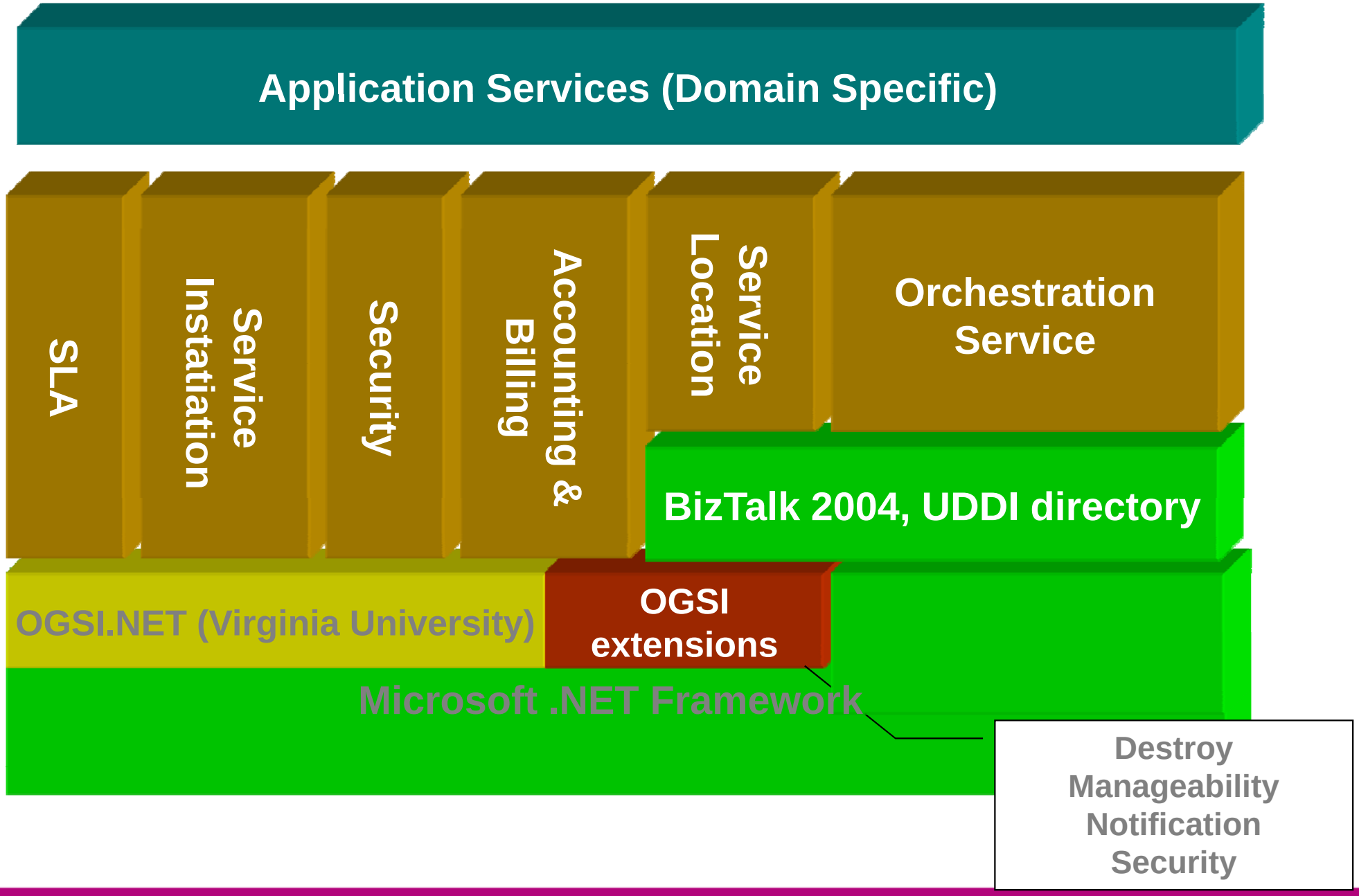
GRID, ASP and Web Services concepts



GRASP Consortium

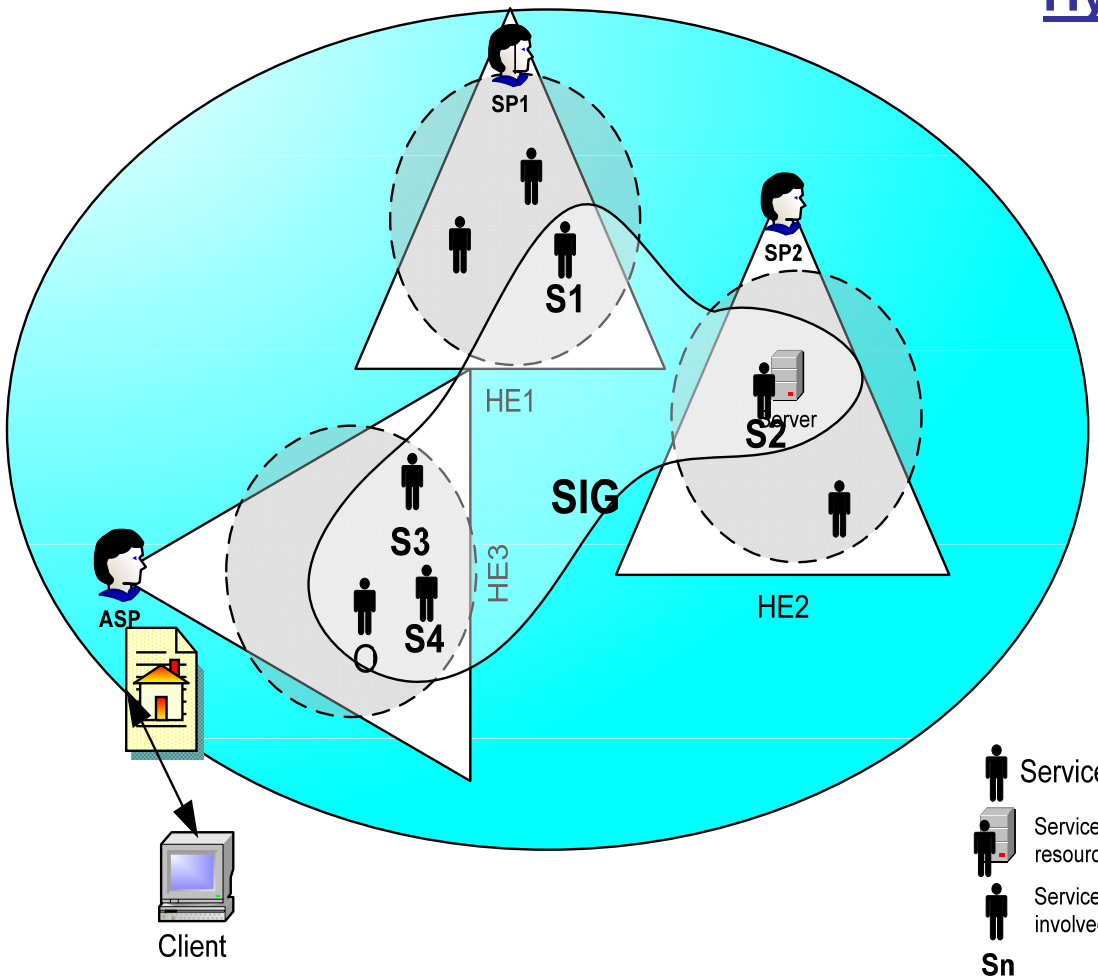
AtosOrigin	(Spain)
CCLRC	(UK)
CRMPA	(Italy)
CSSI	(France)
HLRS	(Germany)
LogicDIS	(Greece)

GRASP architecture overview



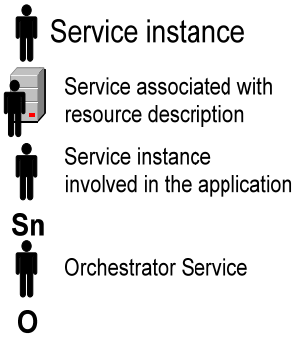
GRASP Security Infrastructure

Dynamic Security Perimeters

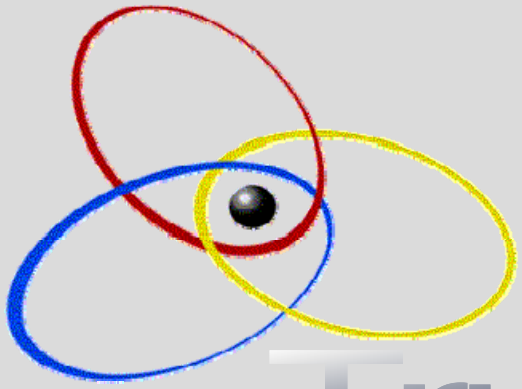


Hybrid Architecture:

- Federated Community Model
- Centralised Administration – per security domain
- 2-layer P2P communication:
  - Admin Level: Policy Management and Negotiation
  - Member Level: CCT Enactment
- Master-slave model for security enforcement



Other activities of interest



TrustCoM

Integrated Project

starts: February 2004
ends: January 2007
funding body: CEC – IST Programme
(Networked Businesses & Governments)

Presenter: Theo Dimitrakos
Affiliation: ISE Group, BITD

Long Term Goal

R&D type

R&D focus

R&D relevance

Technology focus

Business need

To provide a **trust & contract management framework** enabling the definition and secure enactment of

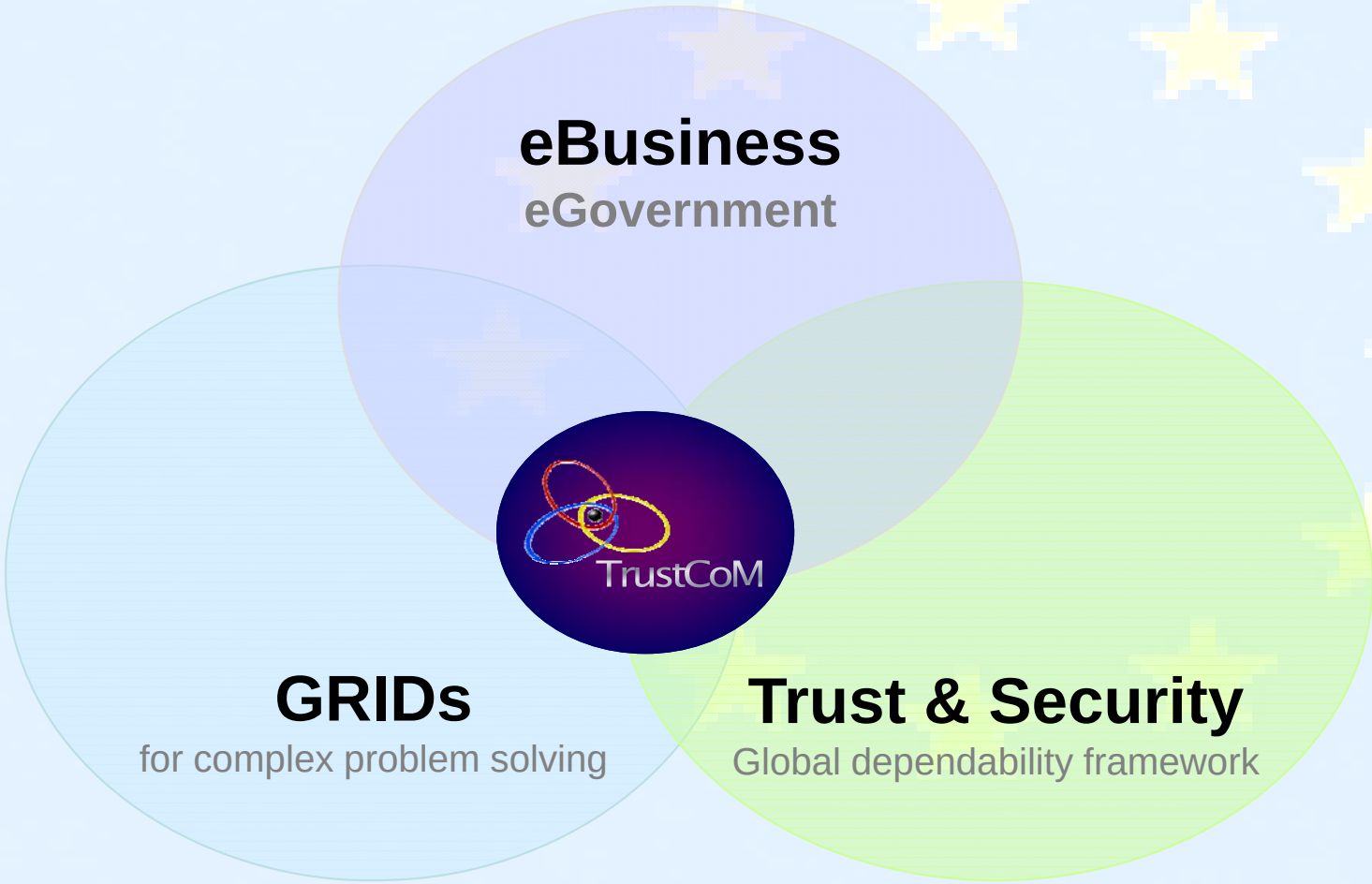
collaborative business processes within **Virtual Organisations** that are formed **on-demand**, are **self-managed** and **evolve dynamically**,

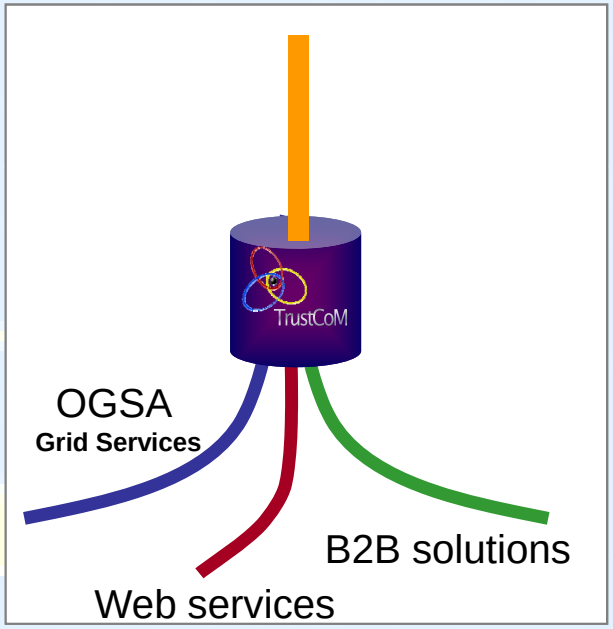
sharing *computation*, *data*, *information* and *knowledge* **across enterprise boundaries**,

in order to

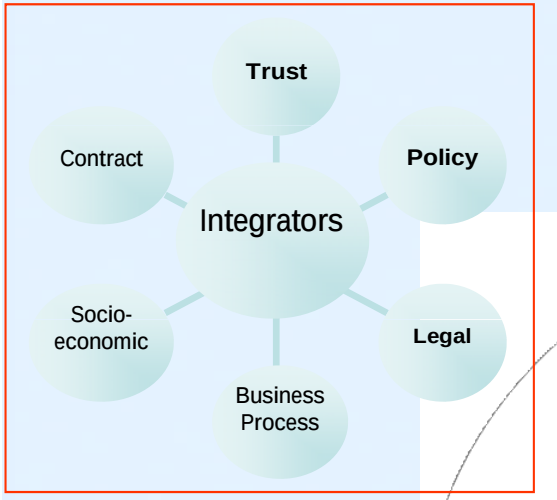
- **tackle collaborative projects** that their participants could not undertake individually or
- **collectively offer** services to customers that could not be provided by the individual enterprises.

TrustCoM position within ERA



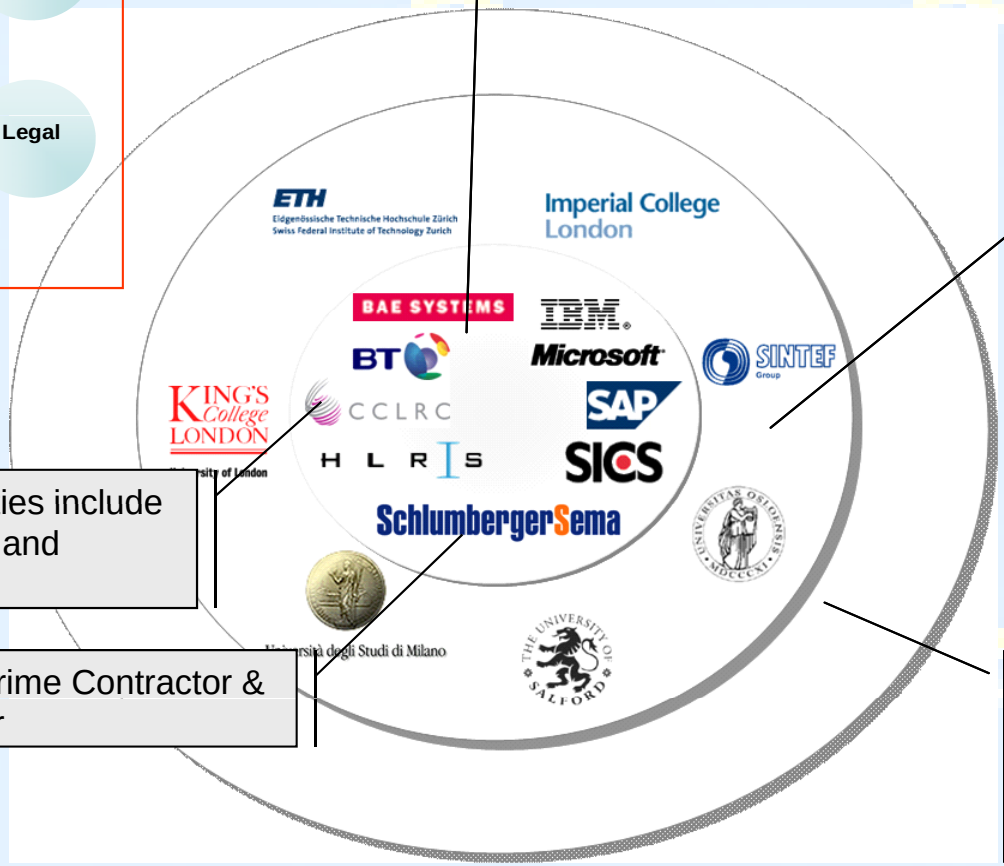


TrustCoM Consortium



Integrators (core group)

Broad knowledge of both technological and research state -of-the art and are capable of blending together research innovation and materialising it into innovative ICT solutions



Technical experts

Sector specific expertise;
will drive research innovation

BITD/CCLRC responsibilities include Programme Management and Scientific Coordination

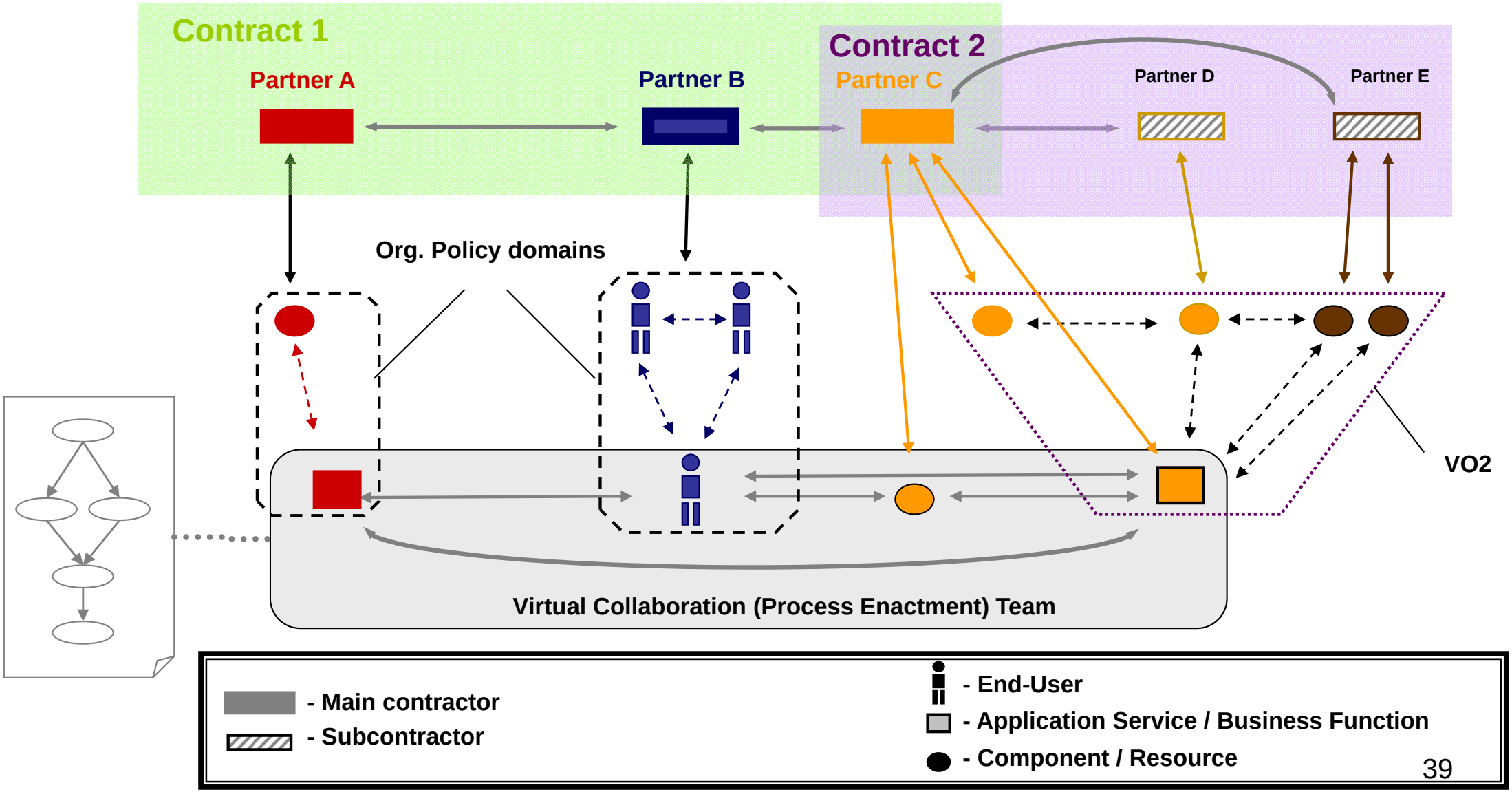
SchlumbergerSema are Prime Contractor & Administrative Coordinator

Advisors

scientific experts and potential user groups;
will be subcontracted to offer consultancy;
will monitor the project progress

Over 10 M Euro overall cost over 3 years --- 6.3 M Euro Contributed by CEC

Targeted Problem via an Example



CCLRC
Rutherford Appleton Laboratory

Other activities of interest

Integrated Project

Starting date 07/2004
funding body: CEC – IST Programme
(Grids for Complex Problem Solving)

Presenter: Theo Dimitrakos
Affiliation: ISE Group, BITD

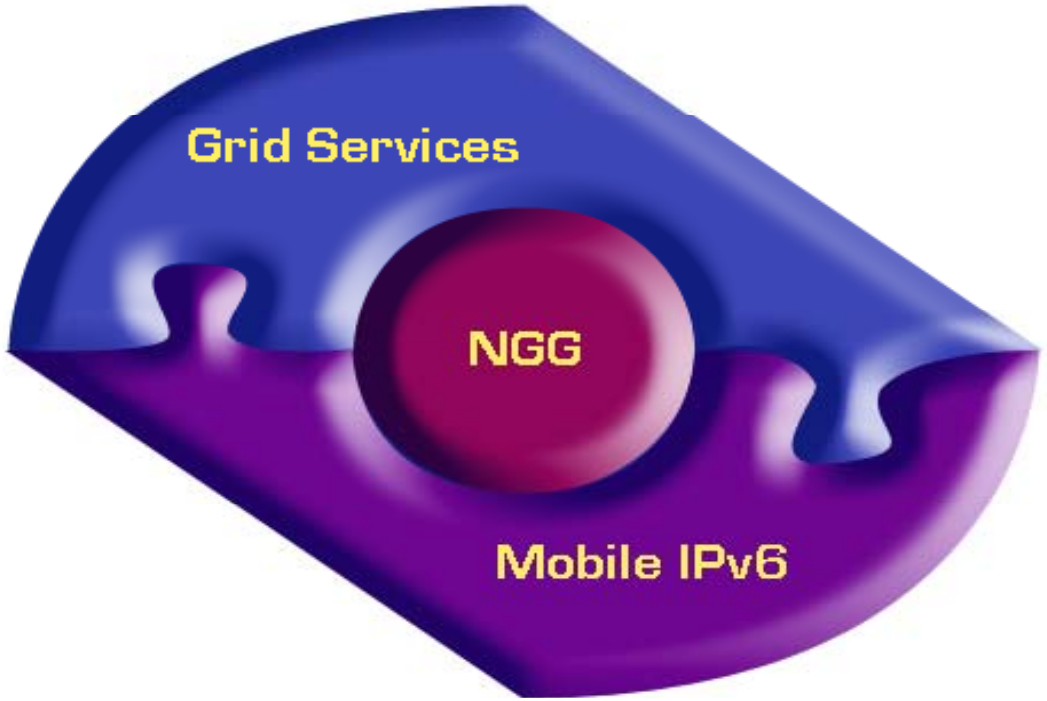
Motivation: signs of times

- **Next Generation Grid needs Next Generation Network**
  - Mobile IPv6 network provide functionality that can be exploited on higher layers (User Profile, Location Awareness)
  - The Grid Middleware has requirements on networks (e.g. QoS)
  - Integrated Security on all layers solve many problems with respect to Trust and securing access to resources
  - The provider concept allow new business and accounting models

The Grid community is about to duplicate to some extent the functionality provided by the Network Middleware of Mobile IPv6

Offers a solution by means of an
innovative integration of Grid and Mobile Computing

Akogrimo in a single picture



- Telefonica (Spain)
- Sema (Spain)
- BOC (Austria)
- Telenor (Norway)
- Datamat (Italy)
- HLRS / Ustutt (Germany)
- UPM (Spain)
- CRMPA (Italy)
- TelInst (Portugal)
- UBwm (Germany)
- CCRLC (UK)
- NTUA (Greece)
- UHoh (Germany)

EC contribution 7M Euros over three years

Motivation: signs of times

- In order to **transform Grid from a niche technology into a self-sustaining technology** it must be:
  - Commercially oriented and ideally integrated into an existing value chain
  - User centric
  - Almost transparent (“the disappearing Grid”)

The Grid community is about to duplicate to some extent the functionality provided by the Network Middleware of Mobile IPv6

Offers a solution by means of an
innovative integration of Grid and Mobile Computing

CCLRC Rutherford Appleton Laboratory

CCLRC

Second International Conference On

TRUST MANAGEMENT

29 March - 1 April 2004
St Anne's College, Oxford UK

An annual event of

itrust

Working group on
Trust Management in
Dynamic Open Systems

www.itrust.uoc.gr

www.trustmanagement.clrc.ac.uk

Supported by

W3C WORLD WIDE WEB CONSORTIUM UK & Ireland Office

www.w3c.rl.ac.uk

2004

Workshop on Formal Aspects in Security and Trust

August 2004, Toulouse (FRANCE)

22nd of August 2004, Toulouse France

– affiliated with the IFIP World Computing Congress 2004

Thank you

Questions?