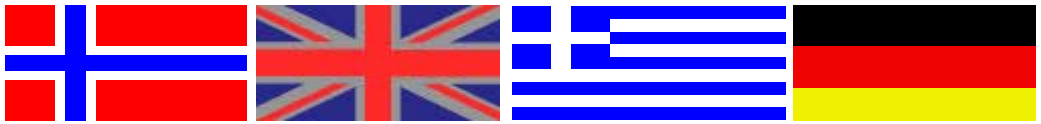
A Platform for Risk Analysis of Security Critical Systems



Model-based Risk Analysis

Targeting Security

Bjørn Axel Gran

Institutt for energiteknikk / OECD Halden Reactor Project

bjorn.axel.gran@hrp.no

CORAS
A Platform for Risk Analysis of Security Critical Systems

Overview

- Introduction
- The CORAS framework
- Model-based risk assessment
  - The CORAS risk management process
  - The CORAS system documentation framework
  - The CORAS platform for tool integration
  - The CORAS integrated risk management and development process
- CORAS trials
- Conclusions

CORAS
A Platform for Risk Analysis of Security Critical Systems

The CORAS Project

- A research and technological development project under the Information Society Technologies (IST) Programme
- Started up in January 2001 and runs until July 2003
- 3 commercial companies:
  Intracom (Greece), Solinet (Germany) and Telenor (Norway);
- 7 research institutes:
  CTI (Greece), FORTH (Greece); IFE (Norway),
  NCT (Norway), NR (Norway), RAL (UK) and Sintef (Norway);
- 1 university college: QMW (UK).
- Telenor administrative responsible
- Sintef scientific coordinator
- IFE responsible for the work package on Risk Analysis

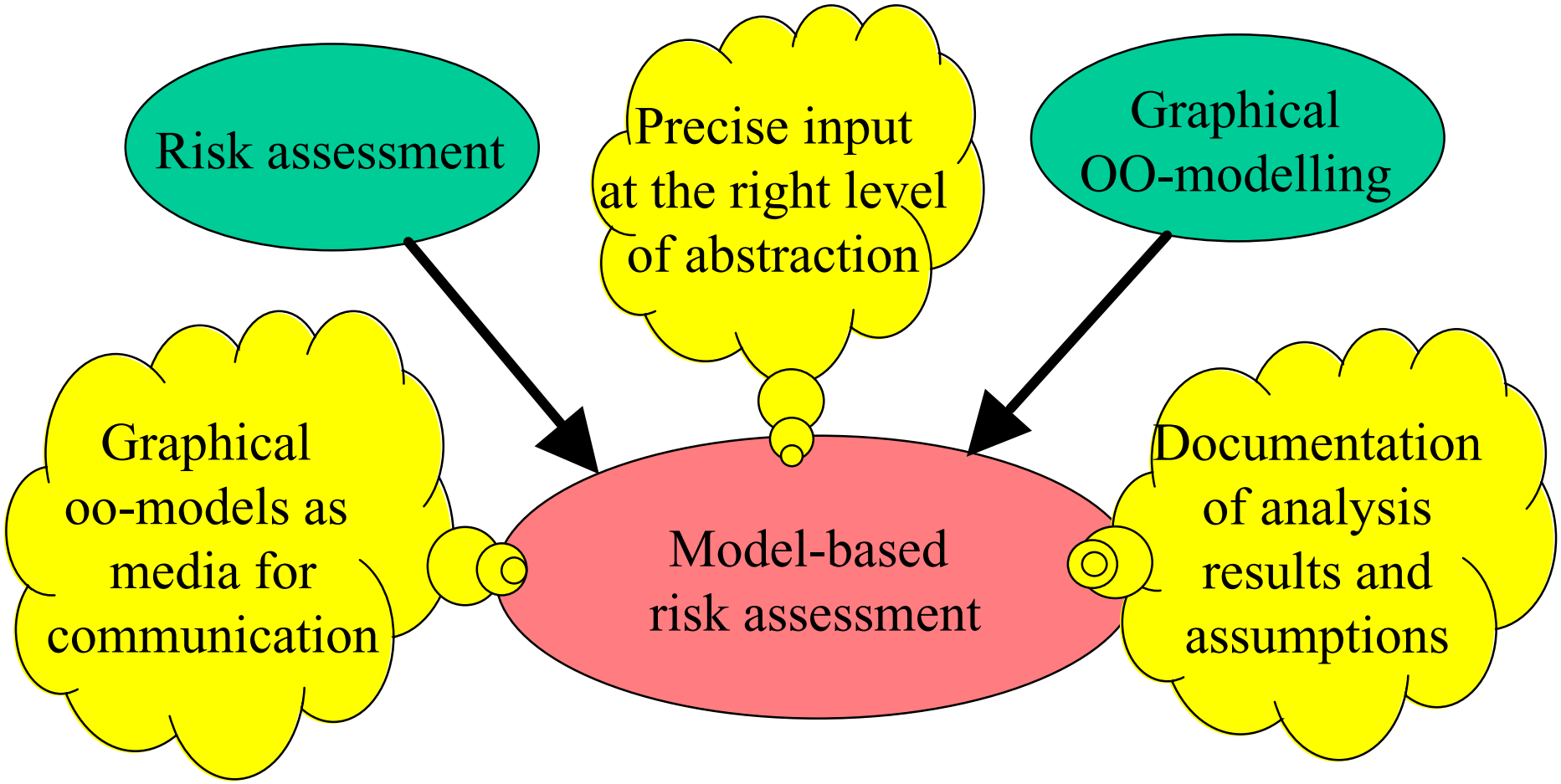
CORAS
A Platform for Risk Analysis of Security Critical Systems

What is CORAS?

- Aims at developing a practical framework for a precise, unambiguous, and efficient risk analysis of security critical systems.
- Exploits methods for risk analysis, semiformal description methods, and computerised tools
- The focus lies on the tight integration of viewpoint-oriented UML-like modelling in the risk management process.
- CORAS addresses security critical systems in general, but puts particular emphasis on IT security.
- Includes all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of IT systems.
- An IT system in the sense of CORAS is not just technology, but also the humans interacting with the technology and all relevant aspects of the surrounding organisation and society.

CORAS
A Platform for Risk Analysis of Security Critical Systems

The CORAS approach: Model-based Risk Assessment



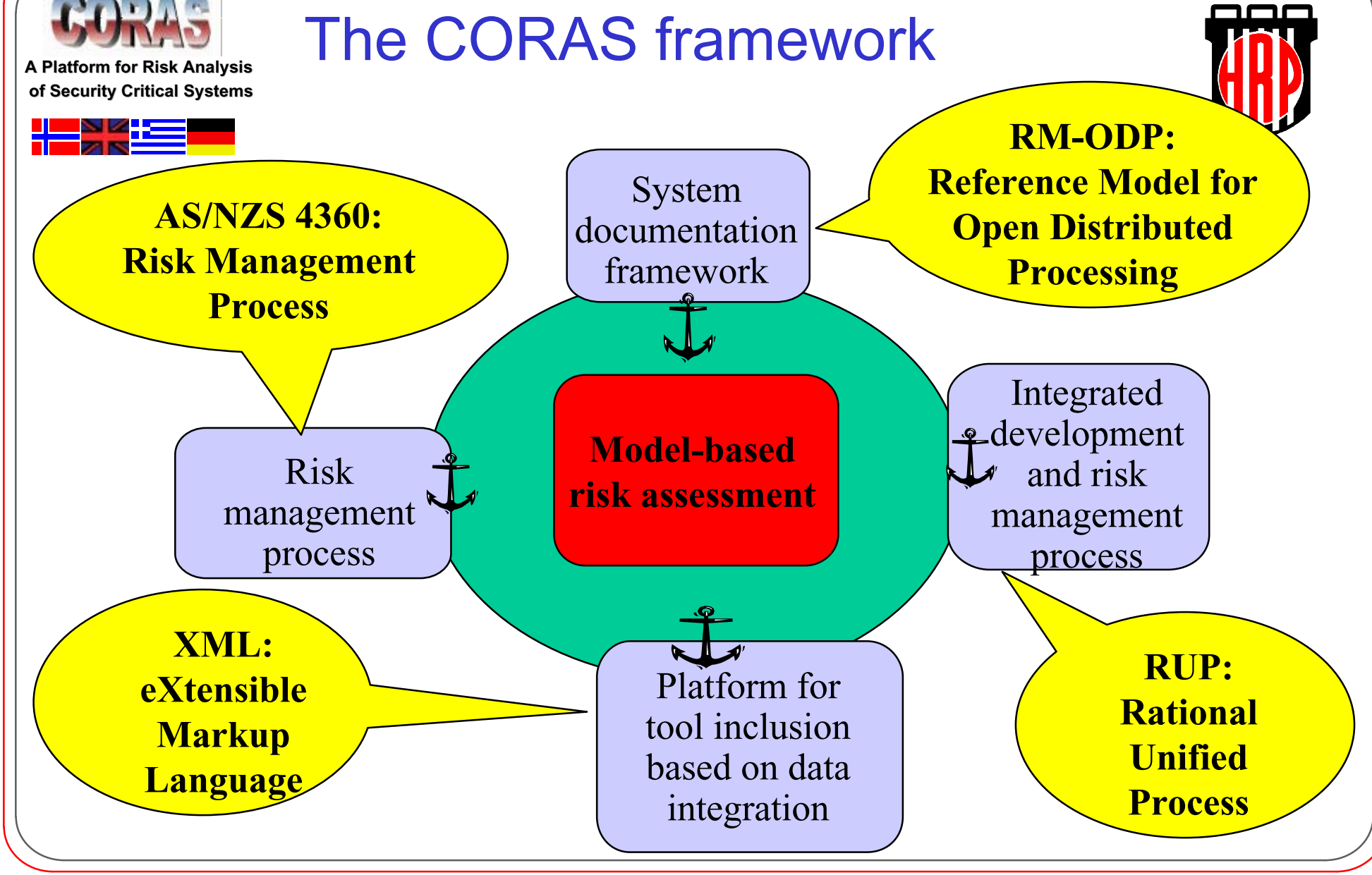
CORAS
A Platform for Risk Analysis of Security Critical Systems

Benefits of Model-based Risk Assessment

- Improved precision in the description of security relevant features **improves quality** of risk analysis results
- State-of-the-art graphical modeling furthers communication between stakeholders, thereby **preventing misconceptions**
- Increased possibilities for reuse **reduces maintenance costs**
- Interoperability between different methods **improves effectiveness**
- Rich set of tools **increases productivity**, efficiency as well as maintenance
- Tight integration of risk management in the system development process **reduces development costs** and ensures that the specified security level is achieved

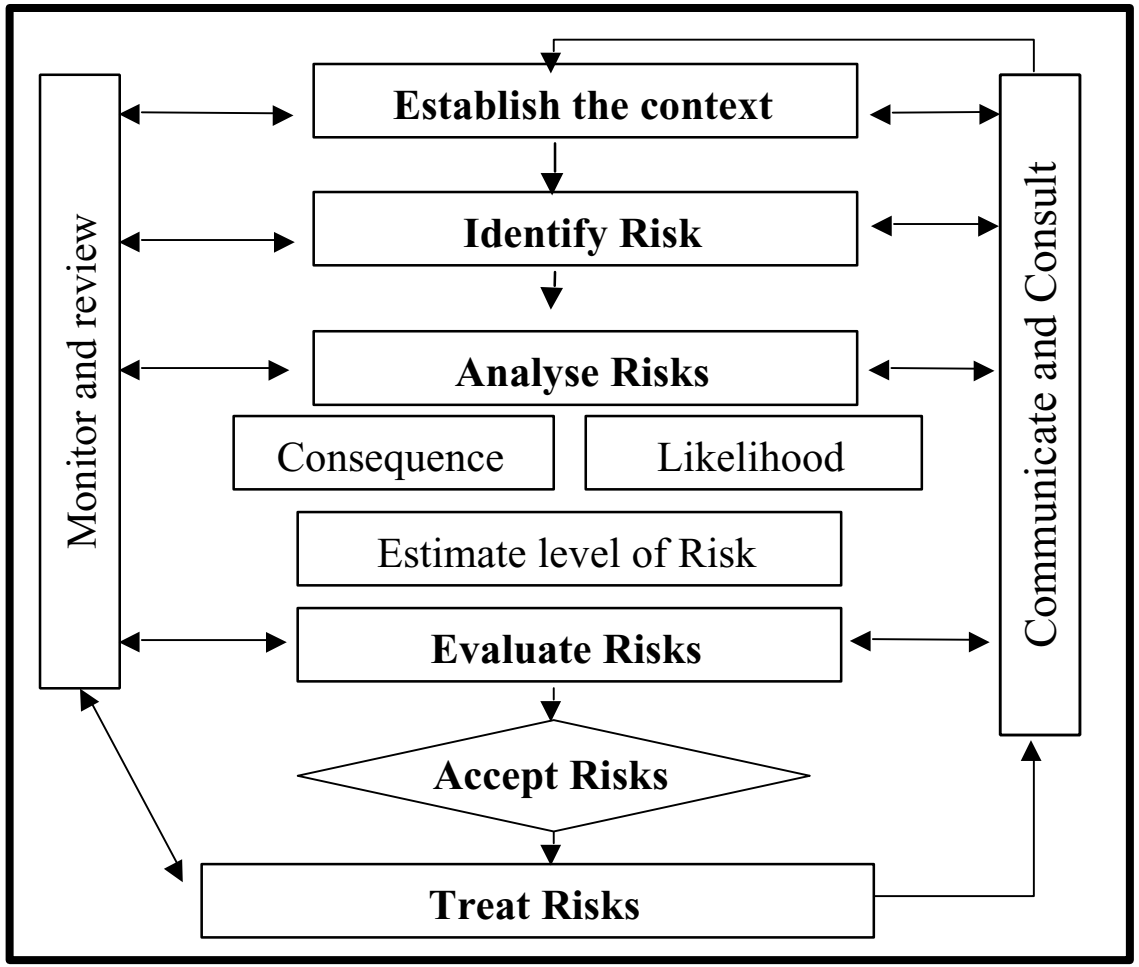
CORAS
A Platform for Risk Analysis of Security Critical Systems

The CORAS framework



CORAS
A Platform for Risk Analysis of Security Critical Systems

The CORAS risk management process



The process is based on

- AS/NZS 4360: 1999 Risk Management
- ISO/IEC 17799-1: 2000 Code of Practise for Information Security Management.

Complemented by:

- ISO/IEC TR 13335-1: 2001 Guidelines for the Management of IT Security
- IEC 61508: 2000 Functional Safety of Electrical/Electronic/ Programmable Safety Related Systems.

CORAS
A Platform for Risk Analysis of Security Critical Systems

The CORAS system documentation framework

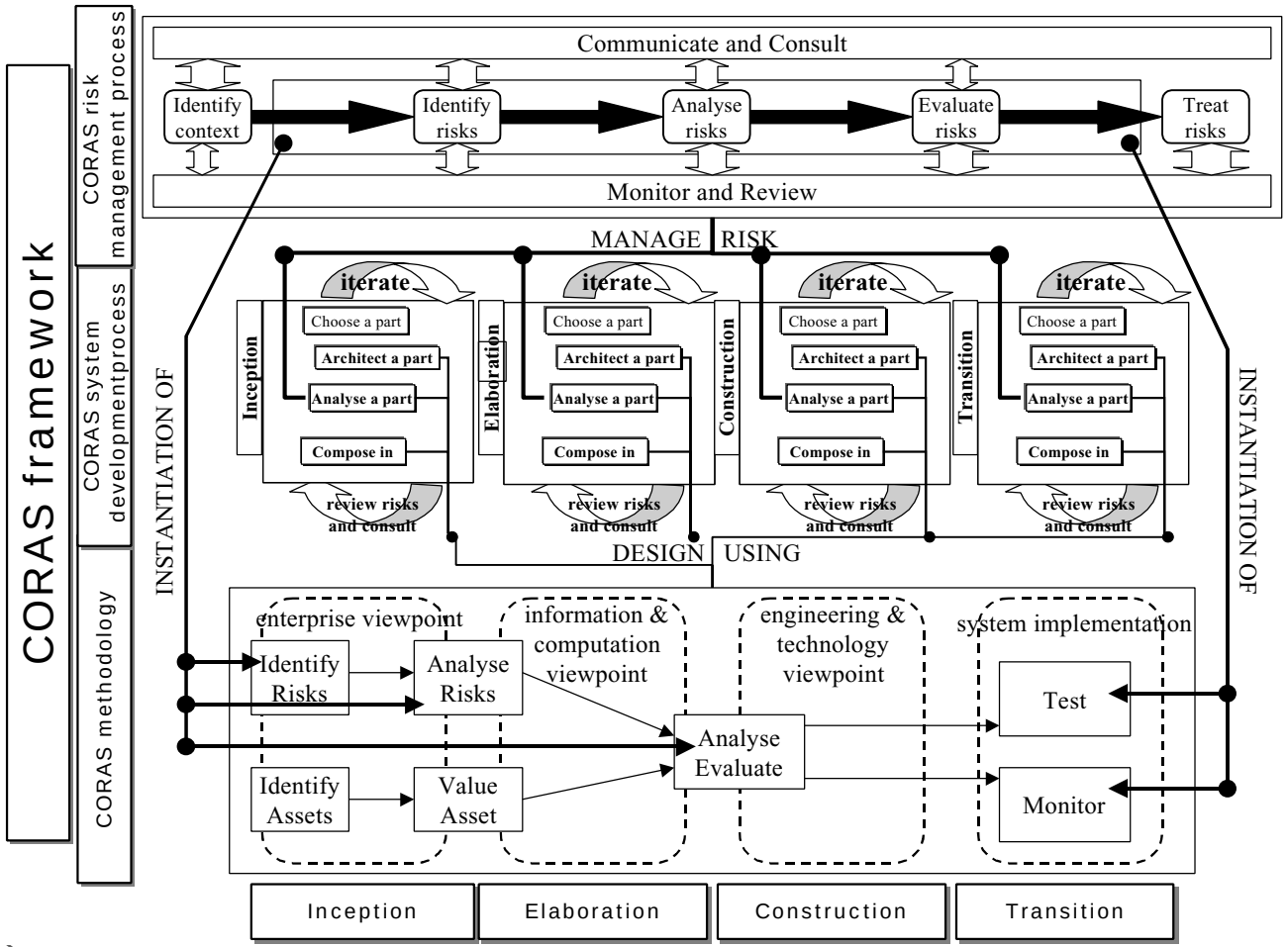
- based on the ISO/IEC 10746 series: 1995 Basic Reference Model for Open Distributed Processing (RM-ODP).
- RM-ODP divides the system documentation into five viewpoints.
- It also provides modelling, specification and structuring terminology, a conformance module addressing implementation and consistency requirements, as well as a distribution module defining transparencies and functions required to realise these transparencies.

The CORAS system documentation framework extends RM-ODP with

- concepts and terminology for risk management and security;
- within each viewpoint carefully defined models targeting model-based risk management and assessment of security-critical systems;
- libraries of reusable model fragments targeting risk assessment;
- additional support for conformance checking;
- a risk management module.

CORAS
A Platform for Risk Analysis of Security Critical Systems

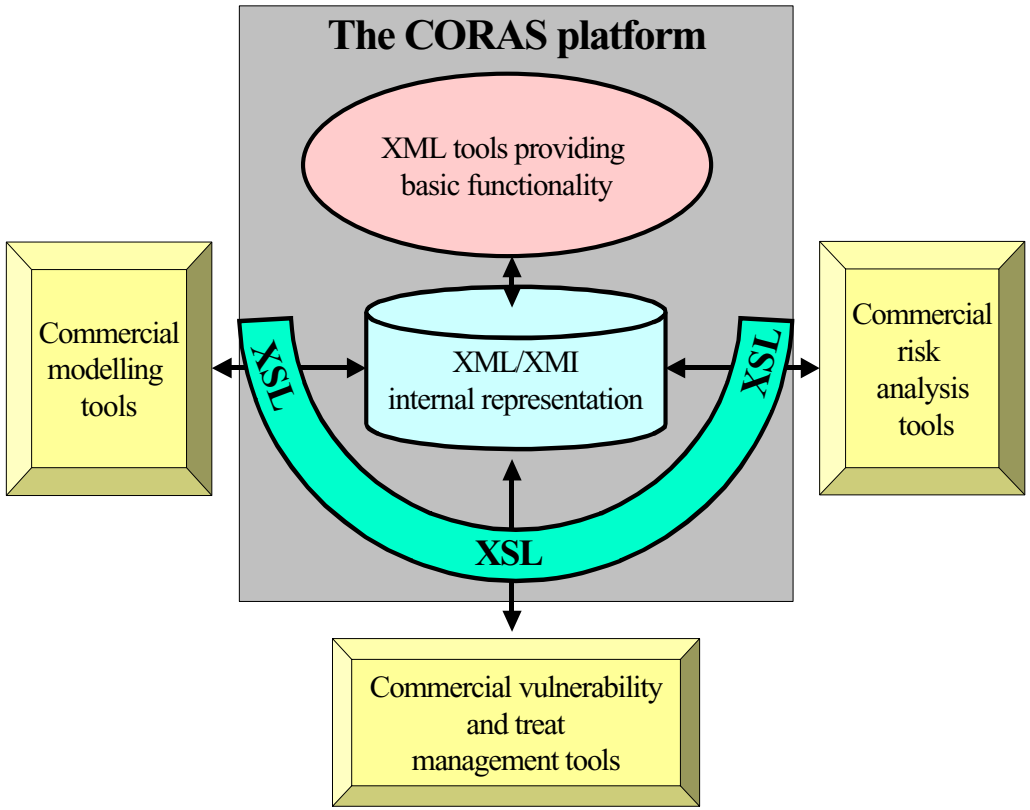
The CORAS Integrated risk management and development process



The CORAS integrated risk management and development process is based on an integration of AS/NZS 4360 and an adaptation of the Unified Process to support RM-ODP inspired viewpoint oriented modelling.

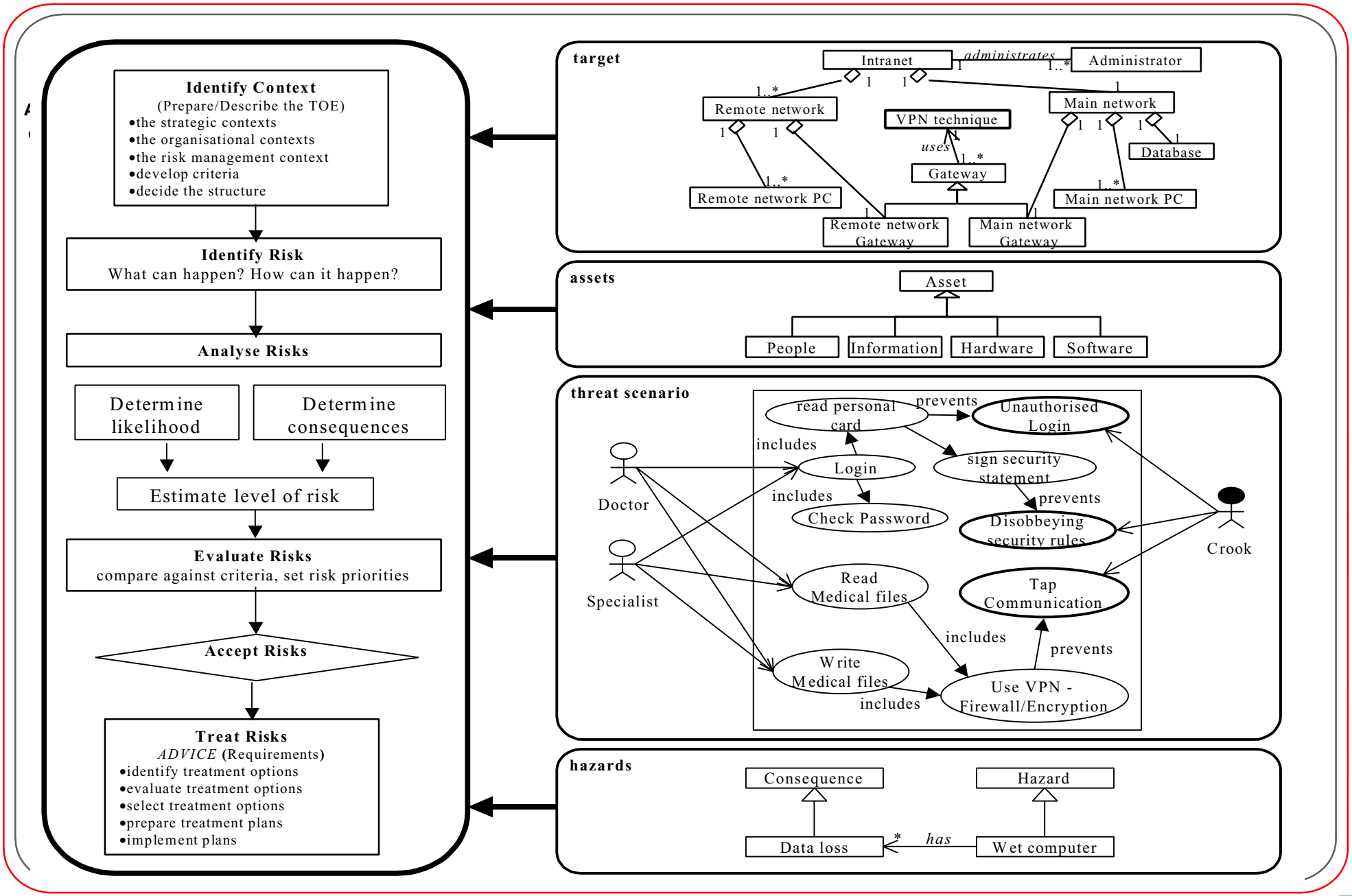
CORAS
A Platform for Risk Analysis of Security Critical Systems

The CORAS platform for tool integration based on data integration



Data integration implemented in terms of XML

- Relevant aspects of the internal data representation may be mapped to the internal data representations (XML/XMI) of other tools.
- This allows the integration of sophisticated case-tools targeting system development as well as risk analysis tools and tools for vulnerability and treat management.


Identify Context
(Prepare/Describe the TOE)
•the strategic contexts
•the organisational contexts
•the risk management context
•develop criteria
•decide the structure
Identify Risk
What can happen? How can it happen?
Analyse Risks
Determine likelihood
Determine consequences
Estimate level of risk
Evaluate Risks
compare against criteria, set risk priorities
Accept Risks
Treat Risks
ADVICE (Requirements)
•identify treatment options
•evaluate treatment options
•select treatment options
•prepare treatment plans
•implement plans
target
Intranet
administrates
Administrator
Remote network
VPN technique
Main network
Database
uses
Gateway
Remote network PC
Main network PC
Remote network Gateway
Main network Gateway
assets
Asset
People
Information
Hardware
Software
threat scenario
read personal card
prevents
Unauthorised Login
includes
Login
sign security statement
Doctor
includes
prevents
Check Password
Disobbeying security rules
Crook
Specialist
Read Medical files
Tap Communication
includes
prevents
Write Medical files
Use VPN - Firewall/Encryption
includes
hazards
Consequence
Hazard
Data loss
has
Wet computer

Sub processes supported by methods

Evaluated methods

Hazard and operability study (HAZOP);
Fault tree analysis (FTA);
Failure Mode and Effect Criticality Analysis (FMECA);
Markov analysis methods (Markov);
Goals Means Task Analysis (GMTA); and
CCTA Risk Analysis and Management methodology (CRAMM).

Sub-process	Recommended Method(s)	Supporting Method(s)
Context identification	CRAMM	HAZOP
Identify Risks	HAZOP, CRAMM	FTA, FMECA, GMTA,
Analyse Risks	FMECA, FTA, MARKOV	HAZOP
Risk Evaluation	CRAMM, FTA	All methods
Risk Treatment	HAZOP	FMECA

The CORAS trials

- In order to ensure the effectiveness and broad applicability of the framework, two architecturally diverse platforms
  - one in the telemedicine and
  - one in the e-commerce domain
- In these trials, in addition to the CORAS consortium, external medical doctors will also be involved in risk analysis tasks.
- The purpose of the trials is to experiment with all aspects of the framework during its development, provide feedback for improvements and offer an overall assessment.
- 3 sub-trials within Telemedicine and E-commerce

The CORAS trials

- The E-commerce platform is a typical Web-based application using Internet technology.
- Availability issues
  - Criticality: Unavailability of a telemedicine platform may have severe consequences resulting in loss of life.
  - Graceful degradation: The E-commerce platform is intended for several users, whereas the telemedicine serves a small number of users. Increase in the number of users may result in degradation of response time.
- Accountability issues:
  - It is important for a telemedicine platform to be able to provide information regarding the access or modifications of data.
- A significant distinguishing factor is the nature of security risks:
  - The E-commerce platform is open to Internet, attracting attackers that probe for weaknesses or opportunities for malicious exploitation,
  - The telemedicine platform operates on a closed network with authorised users communicating using controlled computers.

Software/Hardware developed for the Crete Pilot of the ATTRACT project

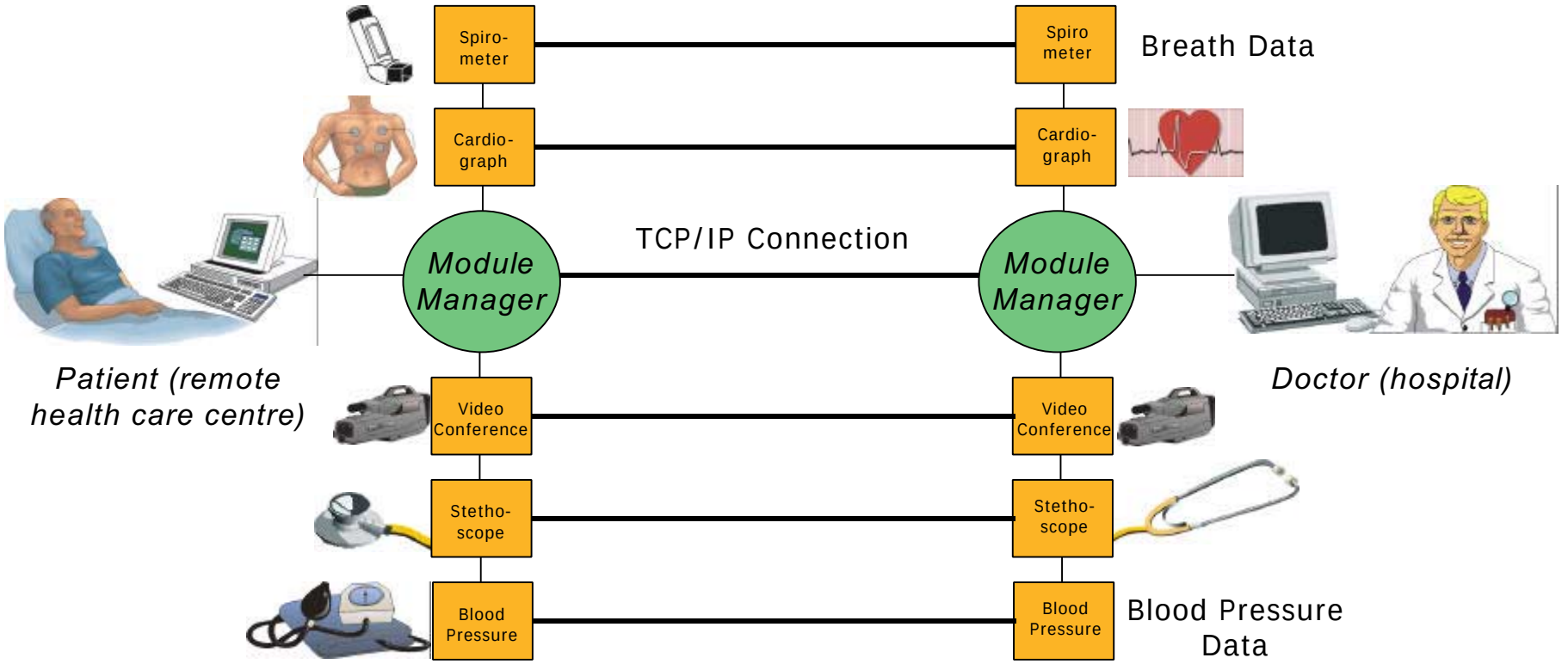
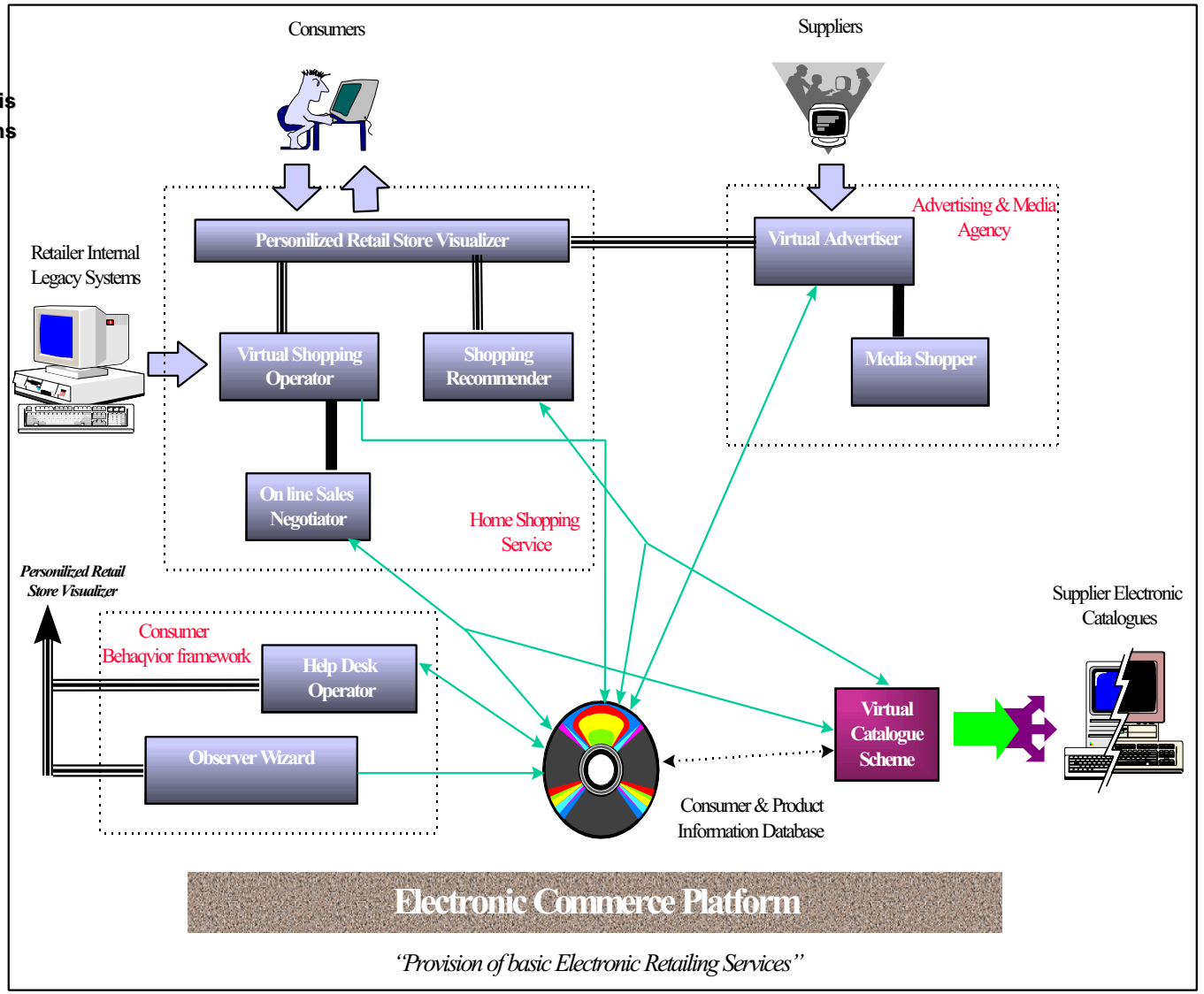
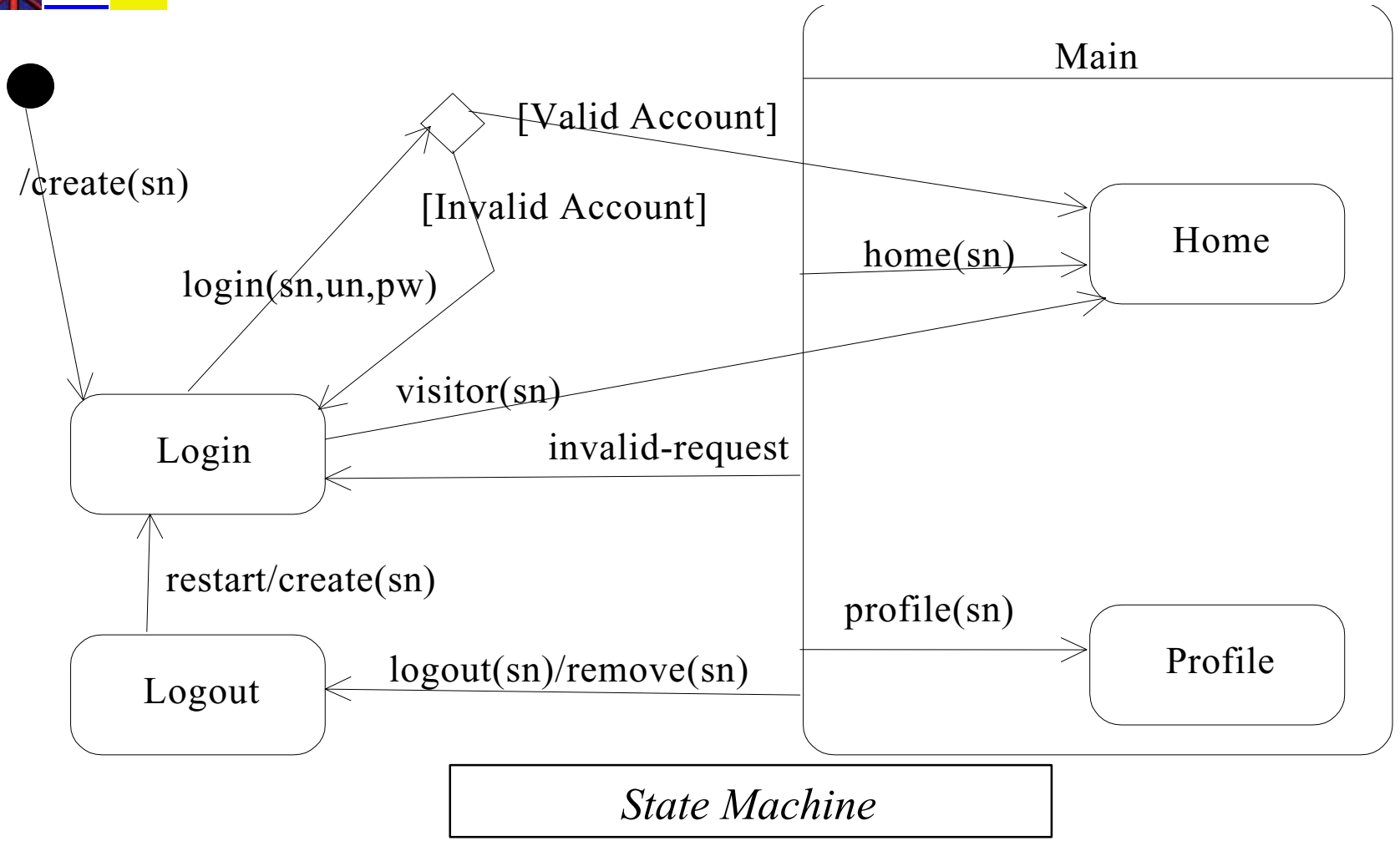


Figure 4: The follow-up scenario of asthmatic children in Crete


Consumers
Suppliers
Retailer Internal Legacy Systems
Personolized Retail Store Visualizer
Virtual Advertiser
Advertising & Media Agency
Virtual Shopping Operator
Shopping Recommender
Media Shopper
On line Sales Negotiator
Home Shopping Service
Personolized Retail Store Visualizer
Consumer Behaqvior framework
Help Desk Operator
Observer Wizard
Virtual Catalogue Scheme
Supplier Electronic Catalogues
Consumer & Product Information Database
Electronic Commerce Platform
"Provision of basic Electronic Retailing Services"
Interconnectivity
Interdependance
Integration
Information flow
Relativity

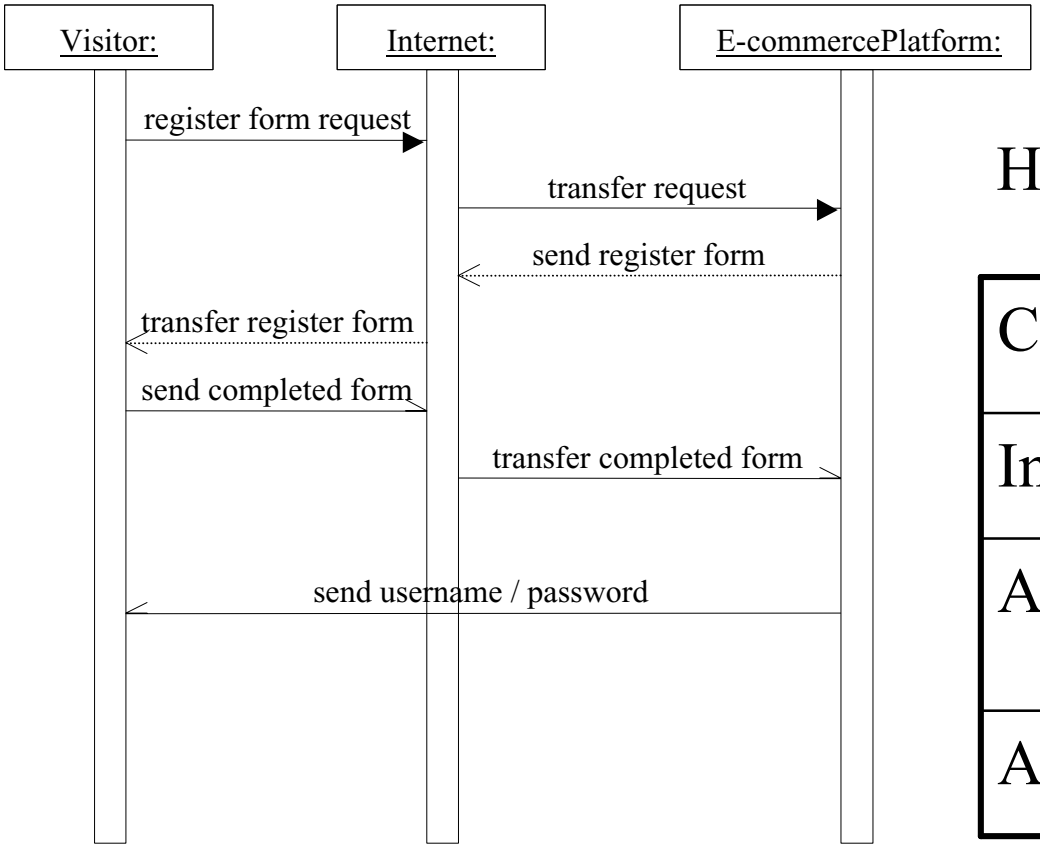
The authentication mechanism



State Machine

CORAS
A Platform for Risk Analysis of Security Critical Systems

Combining RA methods and UML models



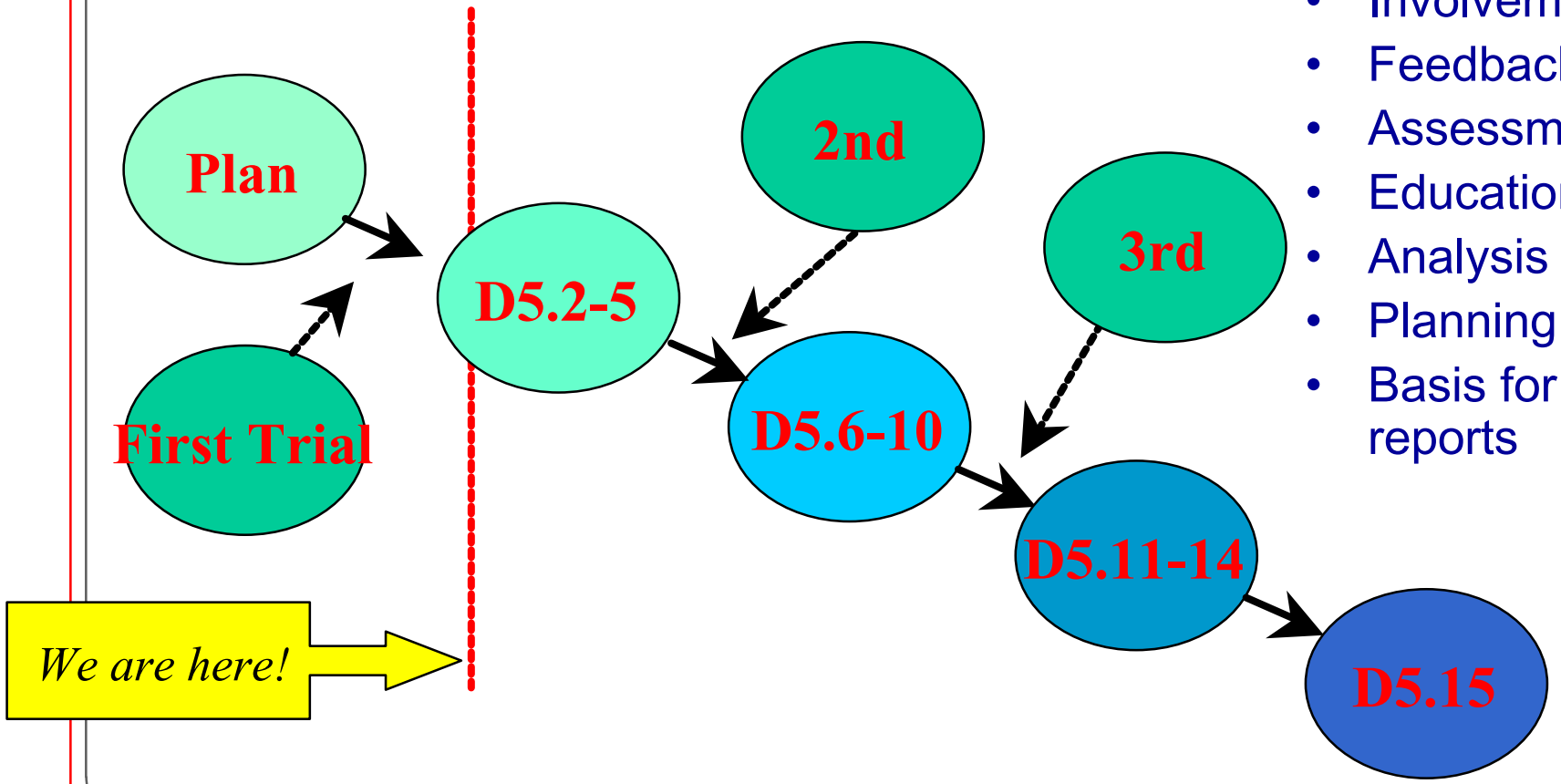
UML Sequence diagram

HAZOP Attributes:

Confidentiality	Disclosure
Integrity	Manipulation
Availability	Denial, delayed
Accountability	Untracability

CORAS
A Platform for Risk Analysis of Security Critical Systems

The CORAS trials
E-commerce



First e-commerce trial

- Involvement
- Feedback
- Assessment
- Education
- Analysis results
- Planning input
- Basis for further reports

CORAS
A Platform for Risk Analysis of Security Critical Systems

Conclusion

- The CORAS framework for model-based risk assessment.
- The CORAS risk assessment methodology integrates aspects of HazOp, FTA, FMECA, Markov Analysis as well as CRAMM.
- It is model-based in the sense that it gives detailed recommendations for the use of UML-oriented modelling in conjunction with assessment.

1. To describe the target of assessment at the right level of abstraction.
2. As a medium for communication and interaction between different groups of stakeholders involved in risk assessment.
3. To document risk assessment results and the assumptions on which these results depend.

CORAS
A Platform for Risk Analysis of Security Critical Systems

Want to know more?

- **www.nr.no/coras**
  - Publications and Public Reports
    … will be updated within short time …
  - Contact Points
    www.ife.no,
    bjorn.axel.gran@hrp.no
- **CORAS Public Workshop**
  - Plan: CORAS workshop at the
  - International Conference on Telemedicine 2002 (ICT2002)
  - www.ict2002.org/, September 22-25 2002 in Regenburg, Germany.