D3C: a coherent, socio-technical framework for identifying, modelling and managing risks in coalition C2

N. Briscombe, P. Goillau, T. Sheppard, G. Watson

A presentation to 11th ICCRTS, Cambridge

28th September 2006

QinetiQ

www.QinetiQ.com

© Copyright QinetiQ limited 2006

Acknowledgements

Based on work funded by UK MOD / RAO ES2 under contract C/CIP/N03506 (Dependable Dynamic Distributed Computing – D3C).

Opinions presented are those of the authors and do not necessarily represent the views of QinetiQ or the MOD.

© Copyright QinetiQ limited 2006

Contents

01 Introduction (P. Goillau)

02 Interoperability frameworks

03 Socio-technical systems

04 D3C research perspective (N. Briscombe)

05 Model development

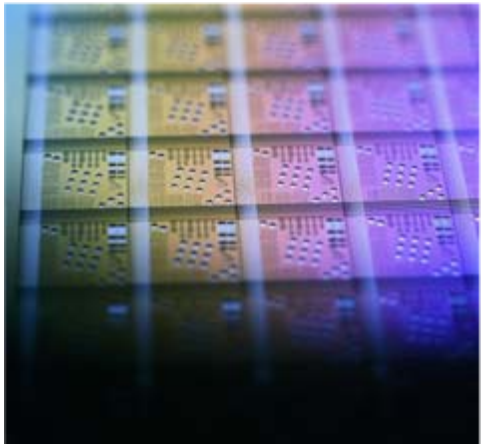
06 Model exploitation

07 Lessons learned

08 Conclusions

© Copyright QinetiQ limited 2006

01
Introduction



© Copyright QinetiQ limited 2006

Introduction

Coalition C2

- Increasingly important
- Increasingly complex
  - Systems of systems
  - Rich, rapidly changing information environment
  - Highly networked C2 architectures – network centric / enabled era

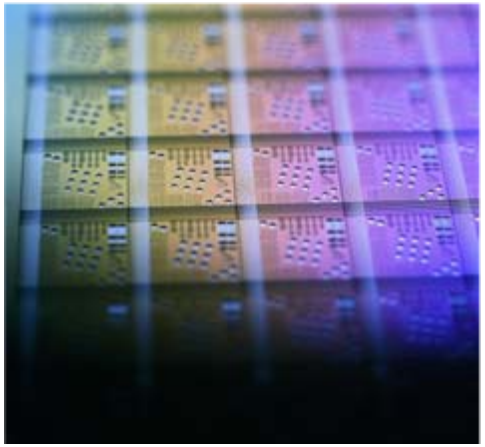
Risks

- Dynamic
- Socio-technical
- Requirement to understand, model, metricate and manage
- Risks include interoperability
  - Underpins inter-working between coalition partners

© Copyright QinetiQ limited 2006

02

Interoperability frameworks



© Copyright QinetiQ limited 2006

Interoperability frameworks

Interoperability dimensions

- Multi-dimensional
  - Not just ‘hard’ technology aspects (interconnectivity)
  - ‘Soft’ human issues (People, process, organisation)
- Security / IA aspects - a key dimension of interoperability (Alberts & Hayes, 2006)
  - D3C specifically addresses the dependability issue, but D3C approach is generic in its wider applicability

Previous interoperability research

- Interoperability frameworks proposed:
  - Technical interoperability
  - Non-technical interoperability (‘co-operability’)
  - Combined interoperability

Pressing need for a single, coherent, socio-technical, dynamic interoperability framework

© Copyright QinetiQ limited 2006

Interoperability frameworks - Technical

Technical interoperability

- Levels of Information Systems Interoperability (LISI) model
  - US DoD framework and structured process
    - Measure, assess and improve interoperability between information systems
  - LISI comprises:
    - Formal Reference Model of interoperability maturity, Capabilities Model, and assessment process
  - The nature of information exchanges are categorised at interoperability levels:
    - Isolated (level 0), through Connected, Functional and Domain, up to Enterprise interoperability (level 4).
  - Implementations at each level are described in terms of four attributes:
    - Procedures, Applications, Infrastructure, and Data (P, A, I, D).
- NATO
  - NATO Interoperability Directive (NID) also strongly focuses on a technology-centric system view

© Copyright QinetiQ limited 2006

Interoperability frameworks - Non-Technical

Non-Technical Interoperability

- NCW emphasises interoperability between forces, not just technologies

- Organisational Interoperability Maturity model (OIM)
  - Maps LISI dimensions onto organisational concerns
  - 4 top-level dimensions
- Multinational forces Co-operability Index (MCI)
  - Extends OIM work with sub-dimensions:
    - Preparedness of organisations and personnel, Understanding – coordination and communication, Command style and structure, Ethos – purpose and culture
    - Numeric risk assessment scale from Unified, through Combined, Collaborative, Co-operative, and Willing, to Independent
- Schade
  - 4 levels of interoperability:
    - Physical interconnectivity, Syntactic, Semantic, Pragmatic

© Copyright QinetiQ limited 2006

Interoperability frameworks - Combined

Combined interoperability

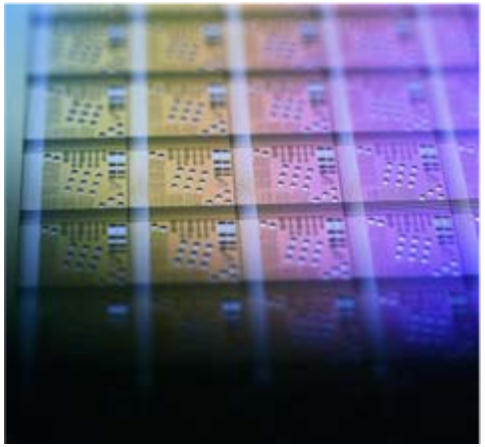
- Layers of Coalition Interoperability (LCI) reference model
  - Facilitates discussion on technical and organisational (political and military) support for interoperable solutions
  - Does not replace other models
- Codner
  - Interoperability as a multi-dimensional concept, extends to joint / multinational military and non-military entities
  - Technical, behavioural (includes organisational / doctrinal, cultural) and logistical interoperability
- Systems of Systems Interoperability model (SOSI)
  - Attempt to integrate technical (e.g. LISI, NATO) and non-technical (e.g. OIM) approaches
  - Software engineering perspective emphasising programme management concerns
  - 3 interoperability levels: operational, constructive and programmatic, requires additional 'environment' level

Must assess interoperability risks from both non-technical + technical network perspectives

- ➔ Socio-technical systems

© Copyright QinetiQ limited 2006

03
Socio-technical systems



© Copyright QinetiQ limited 2006

Socio-technical systems

Four key elements

Trist & Emery (1950s)

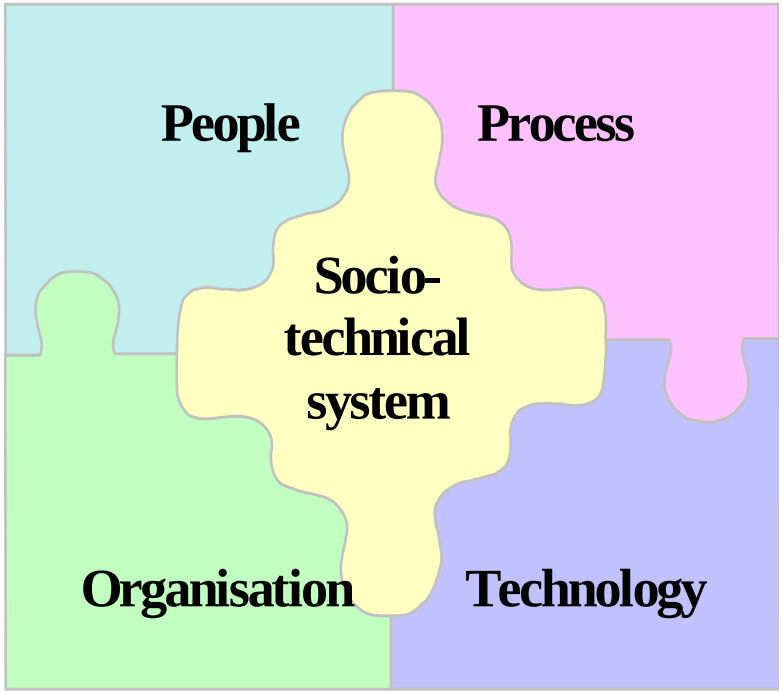
Unique characteristics (Sommerville)

'Invisible architecture'

Hidden power of informal human social networks

Diversity

- Human adaptation supports system diversity
- UK 'Dependability Interdisciplinary Research Council' (DIRC)
- Liaising with D3C



© Copyright QinetiQ limited 2006

Socio-technical systems

Complex human + technology components / interactions

Worthy but disparate past interoperability models

- No single over-arching socio-technical framework

Interoperability dimensions must include security

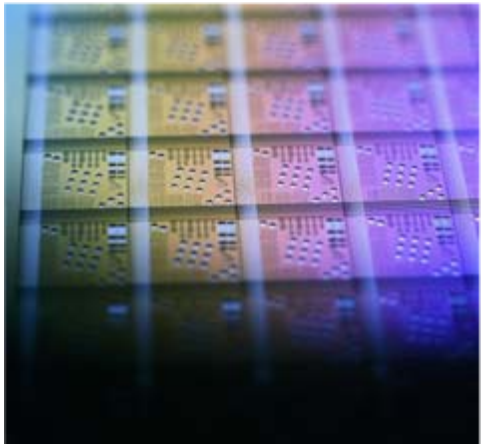
D3C majors on security / IA aspects of interoperability

- We contend security *the* major barrier - focusing on security risk management
- We seek to improve security through models, tooling and enhanced human analysis
- An exemplar single interoperability framework using coalition hierarchies
- Demonstration of applicability of such a framework to IA / security aspects using risk driven process
- Claim that D3C can be usefully applied to the management of general coalition interoperability

- D3C research perspective, model development and exploitation

© Copyright QinetiQ limited 2006

04
D3C Research Perspective



© Copyright QinetiQ limited 2006

D3C Research Perspective - Military Need

Military needs differ from most commercial counterparts

- Adversaries more formidable
  - Hence classification definitions, severe and changing “risk environments”
  - Requirement for robust and flexible risk management
  - A well balanced “Risk appetite” is critical
  - Resolving tension between: information sharing and assurance; in light of the “risk environments”
- Security ≠ access control
  - Military grade analysis **has** to consider **all** forms of compromise
- Accreditation obligation & its burden of evidence

However there are fundamental similarities

- Systems are only necessary means to business goals
- Security can not hamper business goals else security measure are only circumvented

© Copyright QinetiQ limited 2006

D3C Research Perspective - Military Need

Current state of practice

- Knowledge evaporation
  - Document sets intentionally concise
  - Pragmatics motivating concerns and justifications usually non-apparent
  - Intention / intuition to prevent a tendency weighty self obscuring (saturation point)
  - Extremely unhelpful for any attempt of automation

D3C's Technology Development program

- Addresses military need and improves the current state of practice
- Security analysis tool
- Part of a wider Decision Support Tool suite
- Tools engineer semantic models (improving visualization and automation)
- Approach taken also designed to meet future challenges

© Copyright QinetiQ limited 2006

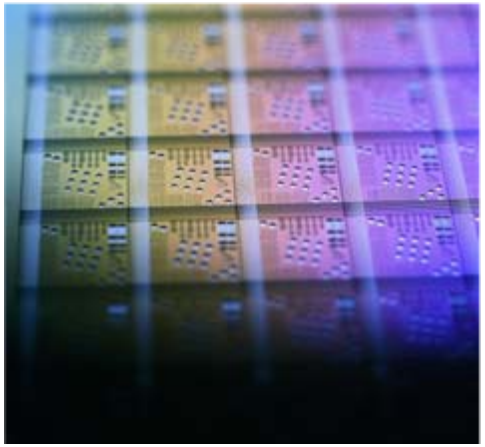
D3C Research Perspective - Technical environment

Technical Environment

- Becoming more complex especially security…
- Visions for future C2
  - “e-defence”, “Power to the Edge”, NEC & NCW
- Increasing scope of technologies employed
  - SOA, Policies, Systems of Systems
- Greater demands
  - Grasp fleeting opportunities, surge capacity
- Evident in NEC themes
  - Agile Mission Groups
  - Inter-working
  - Resilient Information Infrastructure

© Copyright QinetiQ limited 2006

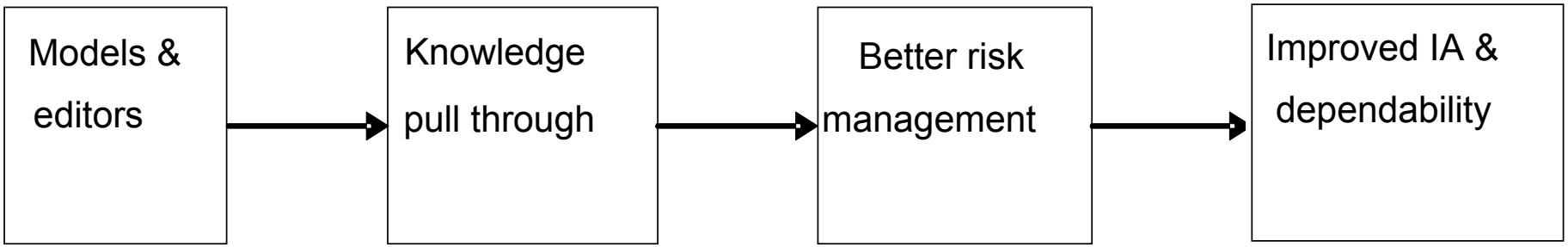
05
Model development



© Copyright QinetiQ limited 2006

Model development

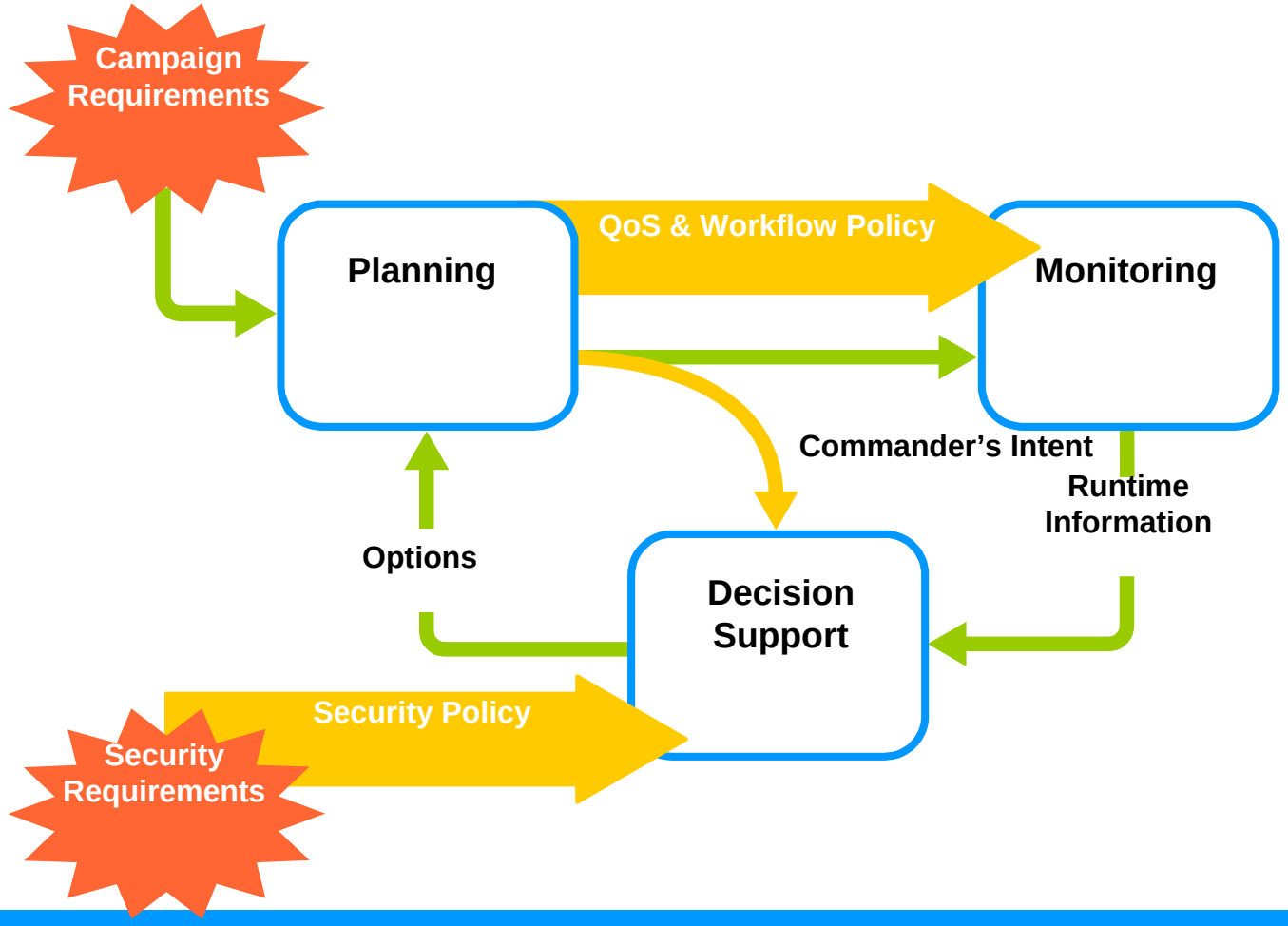
D3C's approach to improving dependability



© Copyright QinetiQ limited 2006

Model development - Technical approach

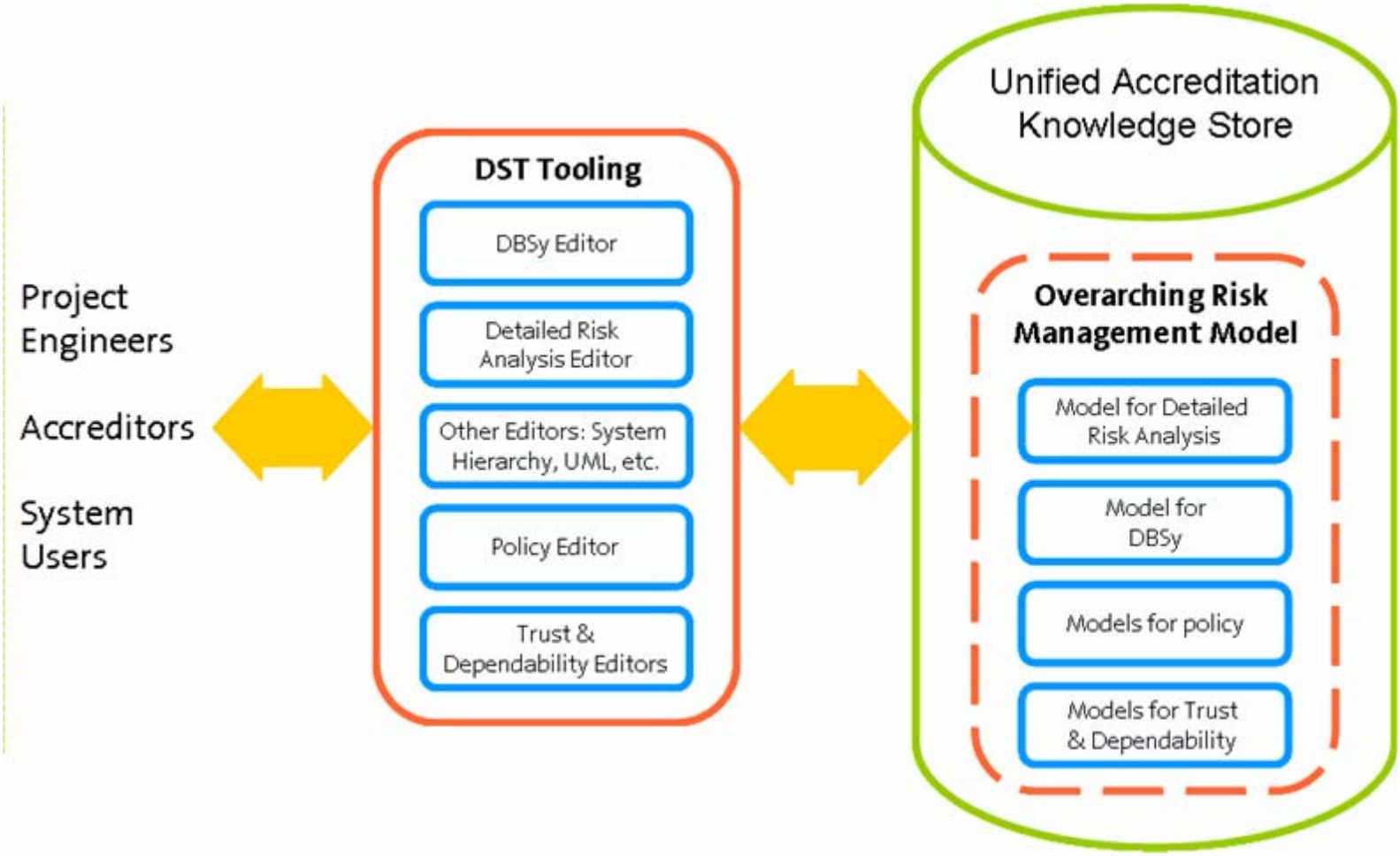
D3C's foci for technology development



© Copyright QinetiQ limited 2006

Model development - Technical approach

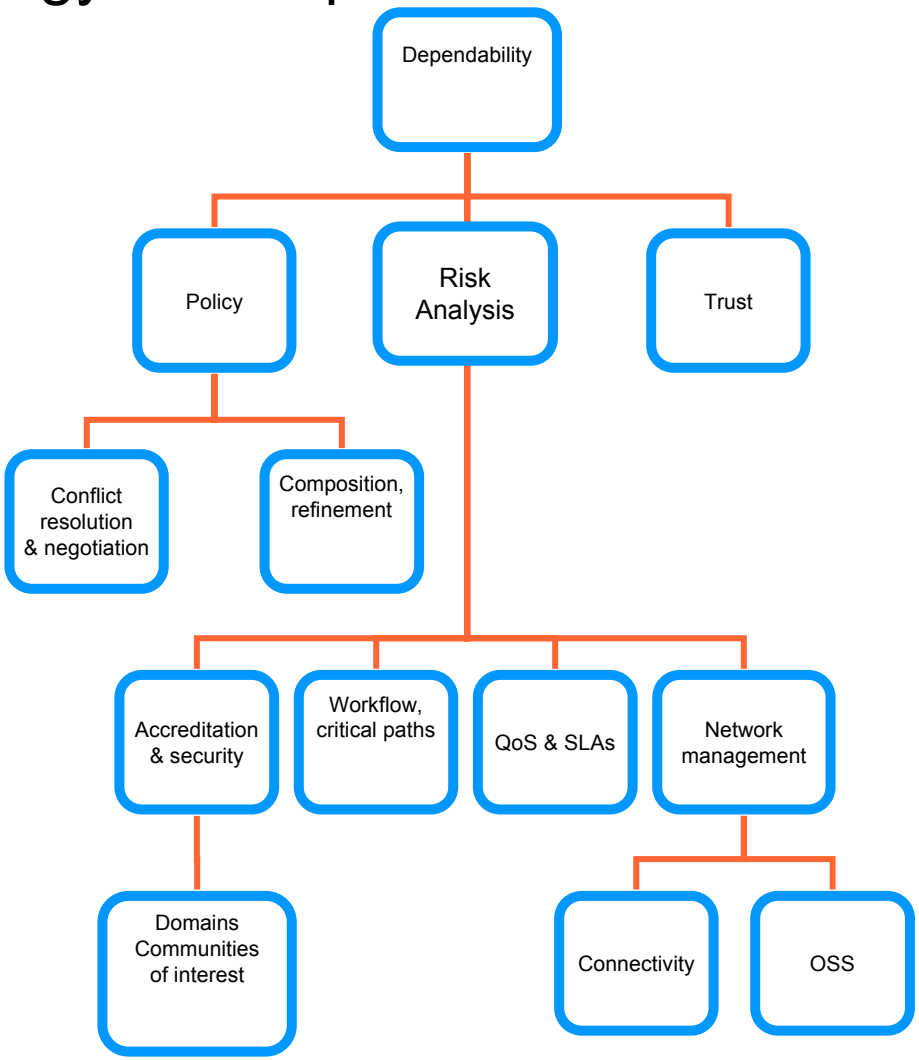
Key models and editors from which the DST is constructed



© Copyright QinetiQ limited 2006

Model development - Ontology Development

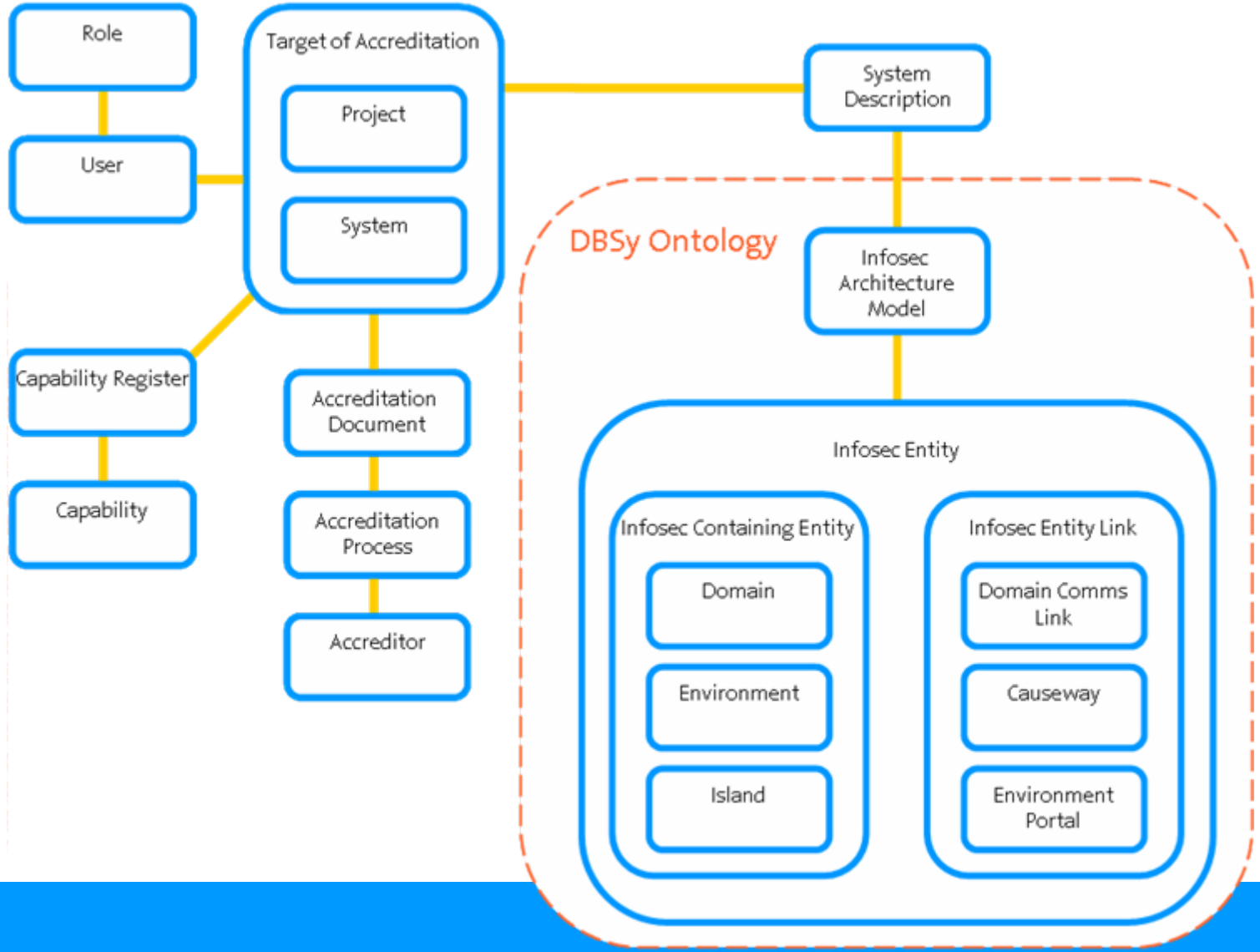
Aspects modelled
in D3C ontologies



© Copyright QinetiQ limited 2006

Model development – Core ontology

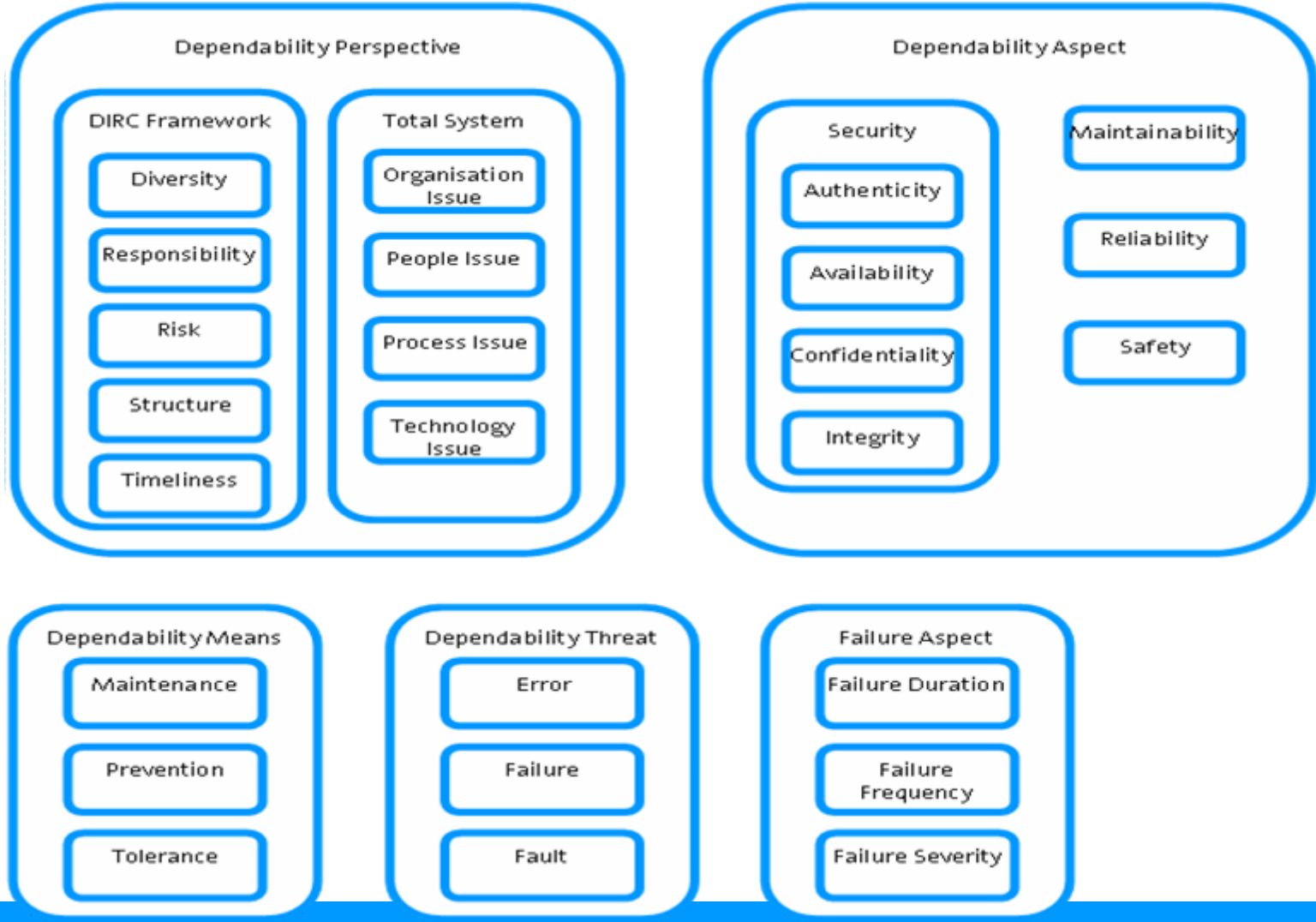
D3C major classes in the 'core' accreditation and DBSy ontology



© Copyright QinetiQ limited 2006

Model development – Dependability modelling

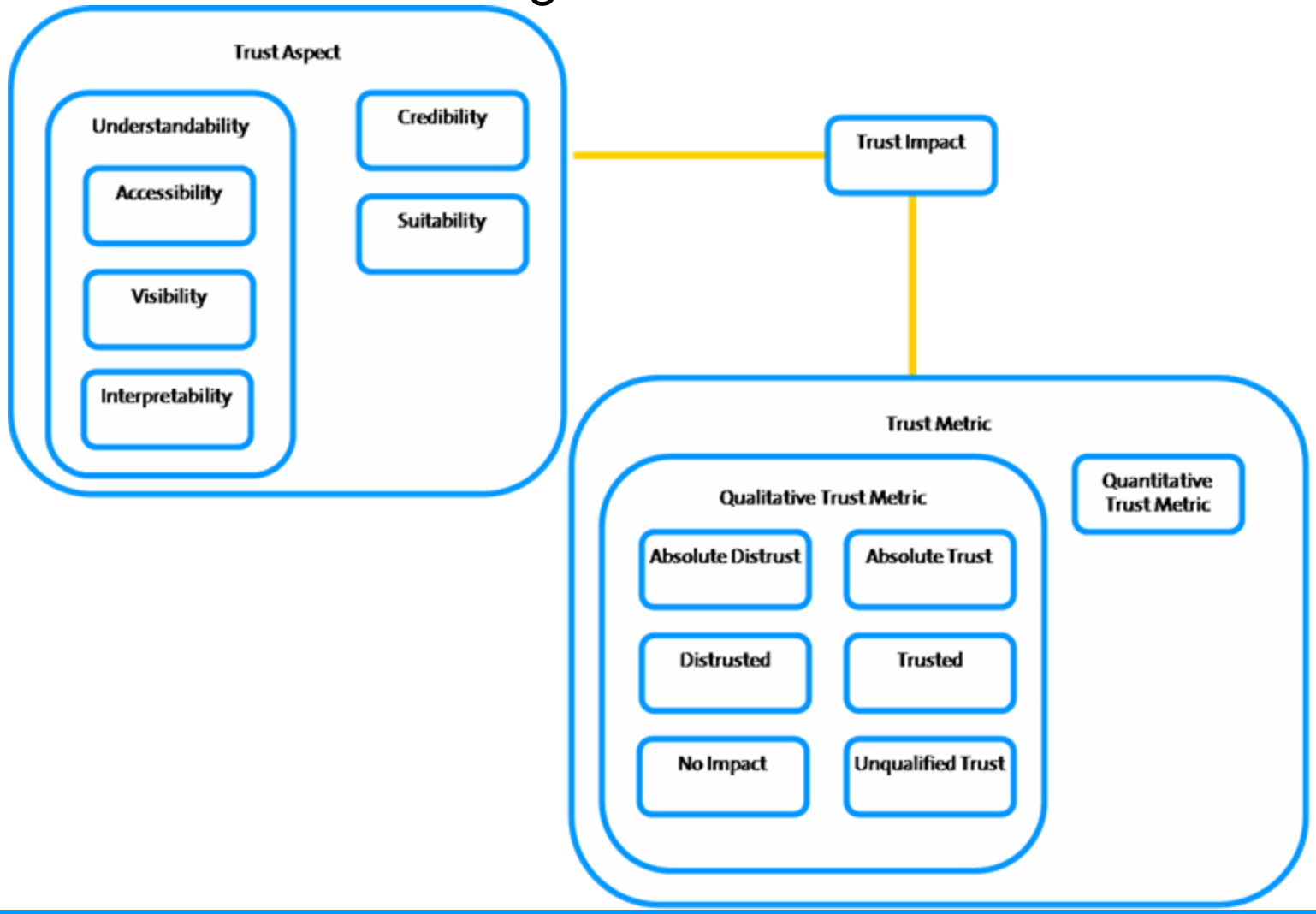
Major classes in the Dependability ontology



© Copyright QinetiQ limited 2006

Model development – Trust modelling

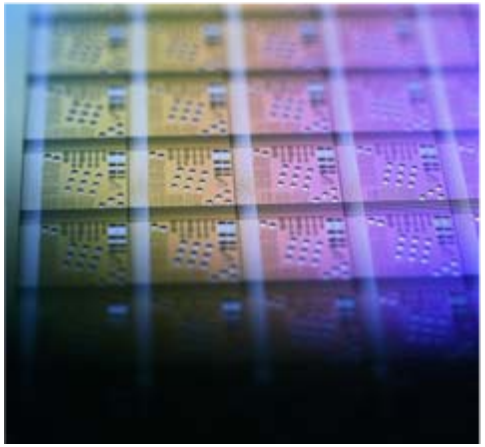
D3C major classes in the Trust ontology



© Copyright QinetiQ limited 2006

06

Model Exploitation



© Copyright QinetiQ limited 2006

Model exploitation - D3C Tooling

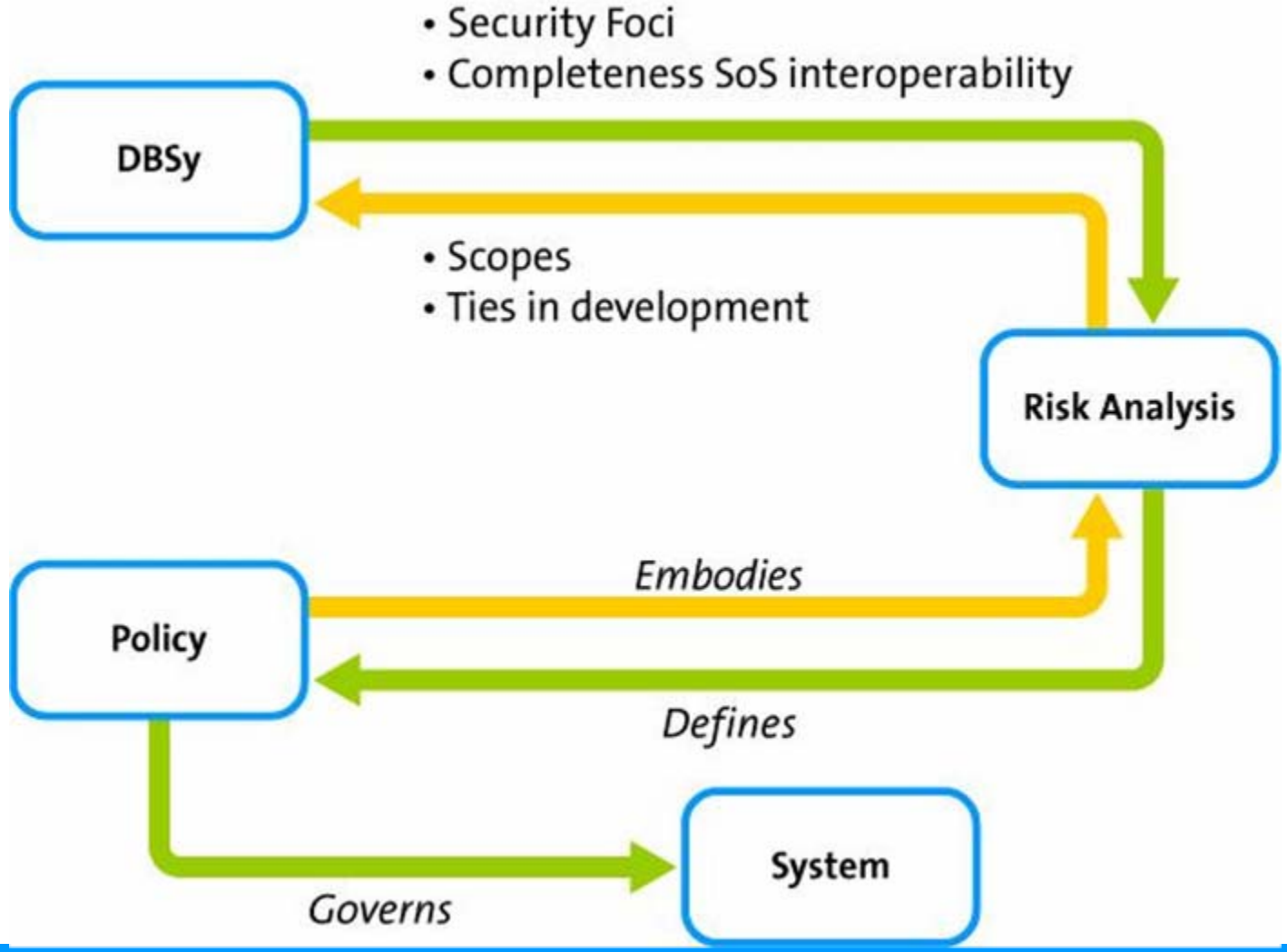
Human-machine interaction table for D3C Tooling

To From	Human	Machine
Human	The tooling allows people to compile, exchange and understand security diagrams and risk analyses	The diagrams and analyses are stored in semantic rich models which are machine readable
Machine	The tooling interprets the models in the knowledge base into diagrams and tables consistent with the current processes in use, which are understandable to people	Systems can exchange models and reason about them, e.g. a system could determine whether to allow communication between it and another system after weighing up the security risks

© Copyright QinetiQ limited 2006

Model exploitation - System governance through policies

Using security risk analysis to govern a system



© Copyright QinetiQ limited 2006

Model exploitation – DBSy editor tool

Develop and navigate complex InfoSec models

- First semantic models for DBSy
- Captures security requirements, boundaries, business information sharing requirements
- Uses current methodologies & nomenclatures
- Shows feasible route to meet future demands
  - e.g. includes Systems of Systems modelling

Stored as a knowledge base

- Some extant tooling support e.g. Protégé for ontology maintenance
- Supports reasoning engines
- Simplifies addition of knowledge domains
- Encourages reflective programming

© Copyright QinetiQ limited 2006

Model exploitation – Risk Analysis & Compromise Path Analysis

Risk Analysis

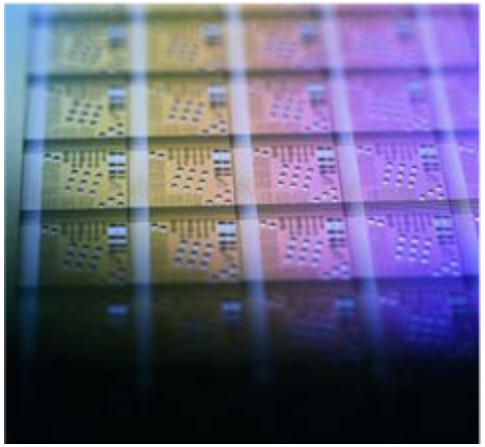
- Breadth of applicability facilitates interoperability
  - CORAS EU IST Risk Analysis
  - Challenges current ethos and practices
  - Perquisite to coalitions in our future settings (c.f. per project analysis)
- Depth of refinement facilitates interoperability
  - Continual, traceable refinement
  - Semi-formalised

Automation & Reasoning

- Models available as OWL / RDF
- Automation includes assisting Risk Assessment process
- Reasoning includes Compromise Path Analysis
  - e.g. finding greatest risks, least/untreated path segments,
  - Searches all possible means and routes of attack

© Copyright QinetiQ limited 2006

07
Lessons learned



© Copyright QinetiQ limited 2006

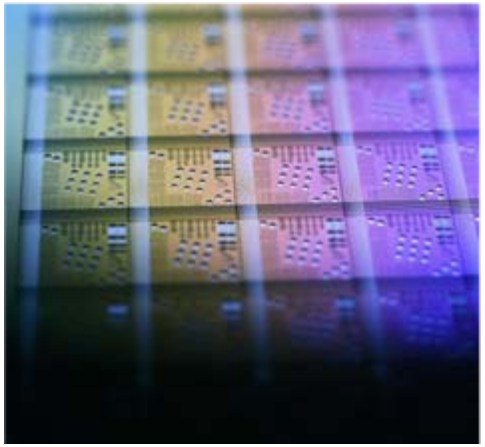
Lessons learned

Lessons learnt so far on the D3C project include:

- A social-technical perspective
- Underpinning technology development with scenario development, practitioners' and experts' workshops
- Developing ontologies with practitioners and researchers
- Ontology development tool such as Protégé
- Ontology development is a continuing process as it must adapt to changes in the outside world if it is to remain salient.
- Modelling can be automatically validated and reasoned upon.
- Model centric view to development
- Implemented in a language that allows introspection / reflection

© Copyright QinetiQ limited 2006

08
Conclusions



© Copyright QinetiQ limited 2006

Conclusions

In this paper we have related key points from the D3C project in the belief that the approach, the modelling framework and the domain knowledge developed under D3C can improve the management of interoperability.

We would warmly welcome discussion with researchers in related fields on this topic.

At our workshops and thought experiment sessions, applying D3C's formalised risk framework generated an enhanced shared understanding of risk factors for the participants.

This facilitates the process of risk re-evaluation in response to changes in our simulated coalition scenarios.

© Copyright QinetiQ limited 2006

QinetiQ

The Global Defence and Security Experts

www.QinetiQ.com

© Copyright QinetiQ limited 2006