11TH ICCRTS
(International Command and Control Research and Technology Symposium)
"COALITION COMMAND AND CONTROL IN THE NETWORKED ERA"
September 26-28, 2006, Cambridge, UK.

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

Suggested session Topics: Coalition interoperability, Network-centric metrics, Information assurance, Social domain issues, Lessons learned.

Name of Author(s):
Neil Briscombe, Peter Goillau, Tim Sheppard and Graeme Watson.

Point of Contact: **Neil Briscombe**

Name of Organization: **QinetiQ Ltd.**

Complete Address: QinetiQ, Malvern Technology Centre, St. Andrew's Road, Malvern, Worcestershire, WR14 3PS, UK.

Telephone: +44 (0) 1 684 54 3844

E-mail Address: njbriscombe@qinetiq.com

Abstract

Previous research has addressed both technical and non-technical interoperability risk factors in coalition command and control (C2). However, there remains a pressing need for a single, coherent, socio-technical, dynamic framework for understanding, modelling, metrication, and management of risks in highly networked coalition C2 architectures. This paper describes how such a framework developed by the Dependable Dynamic Distributed Computing (D3C) project meets this need, summarises the D3C approach to risk assessment and management, and illustrates key 'lessons learned' from its application in simulated coalition scenarios.

D3C's socio-technical, total 'system-of-systems' perspective on risks in C2 information architectures is essential, since risks may arise from people, process and organisational as well as technology network aspects. Coalition C2 also operates in increasingly 'rich' and dynamic information contexts e.g. inter-agency / Non Governmental Organisations (NGOs), implying changing risks which must be managed through dynamic risk mitigation policies.

D3C's approach builds a modelling / categorisation schema ('shared ontology') of risk-related issues, including information, security, technology and human-centred concerns. A decision support tool based on a semantic reasoning engine is used to infer risks and inform accreditable risk mitigation policies. Military scientists can analyse a system's dependability and trustworthiness, whilst end users gain a practical tool for understanding and managing information risks.

Applying D3C's formalised risk framework generated an enhanced shared understanding of risk factors, so facilitating the process of risk re-evaluation in response to changes in simulated coalition scenarios.

1 Introduction

In this paper we relate key points from the Dependable Dynamic Distributed Computing (D3C) project. The purpose of presenting this paper is to confer our belief that the framework and the domain knowledge developed under the D3C programme could be used to improve the management of interoperability in complex systems. The project is split into three courses of work: background studies & scenarios, technology development, and demonstration. Tackling the broad subject area of dependability, we found focus in the security and dynamic risk management of Information Assurance (IA) as the pressing military need. The approach formulated is shown in figure 1.

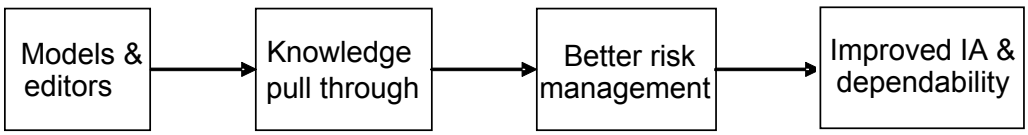

Figure 1: D3C's approach to improving dependability

Section two provides the reader with an explanation of the perspective in which the research is conducted to indicate where our focus was derived from large subject areas.

Section three briefly surveys interoperability frameworks and system models to present the main schools of thought in this area that D3C can complement.

Section four overviews the approach to the modelling, the areas of interest covered, and some of the key classes in our ontologies to indicate the kind of knowledge that can be represented, visualised and reasoned about.

Section five presents two of the editors that comprise the D3C Decision Support Tool, exploiting the underlying shared ontology framework. This shows D3C's contribution to dynamic IA and acts as an exemplar for the benefit that specialised visualisation tools bring to knowledge representations.

Finally we conclude and present lessons learned through the technology development, the experimentation and demonstration undertaken thus far on the project.

2 D3C's Research Perceptive

There are two themes to D3C's research perspective: those issues involving military need and those issues that are due to the changing technical environment that military Command Information Systems (CIS) are increasingly situated within.

2.1 Military Need

Military systems have marked differences from most civilian systems in that the risks faced involve extremely capable, well resourced and determined adversaries, and the assets at stake include the long term national interest and human life. Because of this, MOD systems are required to have their security issues identified, mitigated, accredited and managed. Systems being accredited face a burden of evidence to show that the security requirements have been identified, and that all the risks can be suitably managed at run time. This involves security in its broadest sense, covering all means by which assets could be accessed or compromised from all threat groups. Clearly this scope is in no way catered for by considering access controls alone, which is the usual focus on security in technical communities such as policy based control and those developing Service Orientated Architectures (SOA).

Accreditation documentation is kept intentionally concise, to simplify the accreditation process and the use of the documentation in the field. However this means that the finer details of the accreditors' concerns or their motivations and justifications etc., are not available to system users in the field. System developers can be motivated to falsely narrow the information sharing scope, as it makes accreditation much easier but at the great expense of the utility of the accreditation documentation. Through our experts and practitioner's workshops it was apparent that specific tooling is needed if current security analysis methodologies are to provide a comprehensive coverage of security risks for the more complex security cases which are emerging. A further complication is that very careful consideration must be given to IA because the application of protection mechanisms, if too stringent, tends to become self defeating [1].

These factors led us to the conclusion that a security analysis tool, as part of a wider decision support tool suite, represented the greatest potential impact for military systems to pursue in our technology development programme. This is in line with other expert opinion, for example the use of knowledge management techniques to address security risks was a theme of Lt. General Sir Edmund Burton K.B.E supporting the Central Sponsor for Information in his key note speech at the 2005 Domain Based Security (DBSy®) User Conference.

2.2 Technical Environment

The military need above is drawn from current practice; but clearly technical environments, their security issues, and the demands to share information within coalitions are becoming more complex. Visions for future use of military CIS such as Shadbolt's "e-defence" vision [2], Power to the Edge [3] and the developing NEC [4] and NCW [5] equipment lines both make this military need more acute, and the solutions more problematic. In these visions technologies such as SOA, policy-based control and Systems-of-Systems (SoS) aspire to allow different systems and people to be joined together 'on-the-fly'; as part of a surge capacity to respond to fleeting opportunities for example. Yet accreditation of military CIS will clearly remain a prerequisite. Our studies lead us to believe that in the future technical environment, security accreditation and security risk management in the field will potentially become major barriers for interoperability. Additionally compatible security management between coalition partners can be seen as an important dimension of enabling interoperability.

Thus, there is a clear need for models and tools that aid in the capture and management of complex security issues in these dynamic situations. Without improved understanding of risk by those responsible for systems development no further options for complexity, agility or security will be granted by accreditors.

We set our D3C scenarios against this technological climate for accelerating complexity, demand for dynamism and expected surge capacity of ICT capability coupled with the enduring requirements for accreditation. The D3C scenarios developed included two domestic emergency response scenarios and refinement of existing fictitious coalition scenarios [6] set in 2015. These scenarios provided stretching requirements for dynamic and distributed computing services and controlled information sharing in complex,

mixed-trust environments. These integrate multi-force, multi-nation partnerships and can also include information sharing with Other Government Departments (OGDs) and Non-Government Organisations (NGOs) such as aid agencies. The scenarios were analysed to ensure that technical aspects arising from the NEC vision were well covered, especially those from the NEC themes of Agile Mission Groups, Inter-working and Resilient Information Infrastructure (RII).

Before we present the formulated D3C approach in detail, we first briefly survey the existing interoperability frameworks that we suggest could be further enhanced by work being developed under D3C.

3 Interoperability Framework Survey

In the following brief survey of interoperability models, the approaches can be broadly categorised as emphasising either technical or non-technical interoperability issues with few attempts to synthesise a single, coherent yet practical viewpoint.

Previous research, including papers presented at past ICCRTS conferences, has addressed interoperability risk factors in modern command and control (C2). Working towards seamless interoperability is increasingly important in the context of coalition forces in today's network-centric / network-enabled era. Coalition C2 also operates in increasingly 'rich' and dynamic information contexts, which include inter-agency partnerships and NGOs, implying changing interoperability risks and security concerns which must be managed. To this end, a number of interoperability frameworks have been proposed with the goal of better understanding, modelling and quantifying the range of risk factors involved. It is against the context of these frameworks that we wish to present the D3C approach.

From a technical interoperability perspective, the US Department of Defense (DoD) Levels of Information Systems Interoperability model (LISI) [7] provides a framework and structured process to measure, assess and improve interoperability between information systems, from individual sub-systems through to entire information architectures. LISI comprises a formal Reference Model of interoperability maturity, a Capabilities Model, and an assessment process. The nature of information exchanges are categorised at increasingly sophisticated interoperability levels from 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 of Procedures, Applications, Infrastructure, and Data (P, A, I, D). LISI's interoperability representation schema and common vocabulary facilitate establishment of interoperability standards and cooperative agreements among stakeholder communities. In a similar vein, the NATO Interoperability Directive (NID) [8] also strongly focuses on a technology-centric system view.

However, the NCW-literature stresses that it is the interoperability between forces, not just technologies, which underpins network-centric operating benefits. Several researchers have therefore attempted to extend the 'hard' LISI interoperability concept to address 'soft' Non-Technical Interoperability (NTI) concerns. NTI is also known as 'co-operability' - successfully bridging differences in doctrine, organisation and culture [9]. Building on initial Australian work [10, 11], Stewart et al. [12] addressed the modelling and assessment of NTI in multinational forces. As with Clark's original Organisational Interoperability Maturity (OIM) work, NTI was held to comprise four top-level dimensions: Preparedness of organisations and personnel, Understanding – coordination and communication, Command style and structure, and Ethos – purpose and culture. However, these were each further decomposed by Stewart et al. into a number of sub-factors. A Multinational forces Co-operability Index (MCI) was devised to rate each sub-factor on a numeric risk assessment scale from Unified, through Combined, Collaborative, Co-operative, and Willing, to Independent. By providing a score for each factor, diagnostic assessments can be made either for the multinational force as a whole or between the individual nations involved in the coalition / alliance.

Finally, Schade [13] has recently proposed four levels of interoperability from Physical interconnectivity, via Syntactic, Semantic, up to Pragmatic interoperability. Interoperability may be an issue through communications, procedures, and equipments within coalition operations. Schade notes that the most straightforward problem to solve is physical interconnectivity (i.e. technical interoperability), whereas the broader issues of interoperability are more problematic. Syntactic interoperability implies commonality of exchange standards, command language and processes. Semantic Interoperability aids Shared Situation Awareness, implying both sharing of information and the development of identical interpretation of that information. The common interpretation of command intent, across coalition partners with potentially different ways of operating, reaches the domain of Pragmatic Interoperability. Schade remarks that the

present approach to ensuring Pragmatic Interoperability relies very much on fostering human trust and understanding through pre-operational contact and training. However, it may be necessary to develop additional mechanisms to overcome coalition interoperability difficulties, particularly where increases in operational agility, speed of response and tempo are demanded to achieve network-centric benefits.

As is clear from the preceding approaches, interoperability risks may arise from both non-technical (people, process and organisational) as well as technical network aspects: both must be assessed so that commanders / planners can manage or mitigate potential areas of friction. However, there have been very few attempts to integrate the two viewpoints. Tolk [14] proposed a Layers of Coalition Interoperability (LCI) reference model to facilitate discussion on technical and organisational (political and military) support required for interoperable solutions, but not to replace other models. The lower LCI levels address technical (protocol / data / information) interoperability, and a knowledge/awareness level provides a transition to higher LCI organisational interoperability issues (alignment of procedures, operations, doctrines and objectives).

Codner [15] notes that interoperability is a multi-dimensional concept. Joint and coalition services need to be interoperable at many levels: technical, behavioural (includes organisational / doctrinal, cultural) and logistical. Interoperability also extends to both joint / multinational military and non-military entities. Technical interoperability involves attaining interconnectivity between communication and information systems and other services. Behavioural interoperability means responding to a military situation in the same way, and includes doctrinal and cultural aspects - both influenced by constitutional, legal and customary factors. Doctrinal interoperability is closely linked to military strategic concept, and includes guidance relating to information sharing. Cultural interoperability has the greatest impact at the lowest, tactical levels of war e.g. language, work ethic, individual stamina, standards of living, religion and discipline. These are helped though regular proximity, regular training, operating together and through language training. Logistic interoperability involves the ability to provide and accept logistic services such as fuel, spare parts, ammunition, medical services and transport.

The Systems of Systems Interoperability model (SOSI) [16] represents a further attempt to integrate technical (e.g. LISI, NATO) and non-technical (e.g. OIM) approaches, albeit from a software engineering perspective emphasising programme management concerns. SOSI proposes three interoperability levels: operational (interoperability of Conops and protocols between operational systems), constructive (interoperability of mechanisms between the organizations that are responsible for the construction and maintenance of a system), and programmatic (interoperability between different programme offices). SOSI's strength is in usefully addressing the full scope of interoperability from a 'System of component systems' perspective. However, SOSI's programme focus requires an additional 'environment' level to accommodate such issues as policy and standards development. Other valid perspectives such as people-centric or lifecyle-centric also raise relevant issues which are orthogonal to the SOSI approach.

Despite the disparate efforts summarised above, there remains a pressing need for a single, comprehensive approach to address interoperability risks. As part of the work conducted under the D3C project, a modelling framework is being developed which adopts a socio-technical, System-of-Systems perspective to cover a full range of technical and non-technical risk factors in C2 information architectures. A socio-technical system is "an approach to complex organisational work design that recognises the interaction between people and technology in workplaces" [17], where a system's technical and human / social aspects are tightly interconnected. A technology viewpoint alone is insufficient. The original socio-technical system concept was developed in the 1950's by Trist and Emery at London's Tavistock Institute [18-20], to explain why the introduction of coal industry mechanisation had actually led to a decrease in productivity. Figure 2 indicates the four key component elements of a socio-technical system: people, process, organisation and technology.

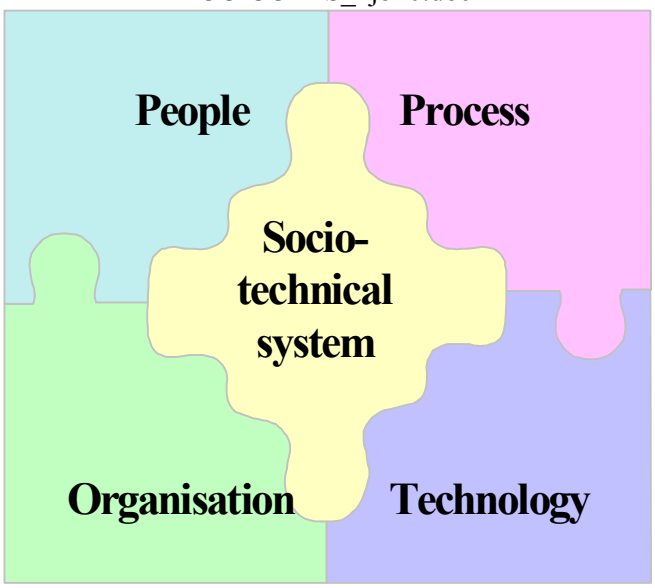

Figure 2: The socio-technical systems perspective.

There has been a recent, renewed interest in socio-technical approaches from the technology-centric community. Dillon [21] remarks that socio-technical systems have found wide application in the information systems domain, complementing the practical focus of usability engineering with a more generic consideration of user motivations and drives.

Sommerville [22] notes that socio-technical systems have unique characteristics compared to pure technology systems, including emergent properties (both functional and non-functional), non-determinism and organisational objectives underpinning complex relationships. Ure and Jaegersberg [23] reinforce the point that "the biggest problems faced by those involved in designing, managing and integrating networked systems are often not technical – they are socio-technical." This 'invisible architecture' of human and organisational issues can seriously hinder a technology-based solution if not fully considered and integrated as part of the development process.

Sommerville is a principal investigator in the Dependability Interdisciplinary Research Council (DIRC) comprised of City, Edinburgh, Lancaster, Newcastle and York universities and funded by the UK Engineering and Physical Sciences Research Council (EPSRC). D3C has also collaborated with Sommerville and his team in Lancaster and Andersons' team in Edinburgh. DIRC was extremely relevant to D3C as it sought to improve IT systems by recognising dependability as a socio-technical property. This is considered to be the combination of the system and the environments in which it was procured, developed and used.

It is intended that the D3C project team will be members of the follow-on consortium from DIRC providing scenarios and case studies with strong challenges for emerging technology in dependability. We will work closely on research and continue our joint experimentation in simulated high dependability environments. D3C is assimilating and refining domain knowledge developed by Sommerville's team [24].

The initial focus of the D3C project is to provide tooling to aid the understanding and mitigation of security risks engendered as a result of changes in the configurations of complex running systems. The tooling which has been developed shares this focus on security and risk analysis, however the project has adopted a very broad approach in modelling the *dependability* of systems, of which the security considerations are only one facet. This underlying framework has been designed to offer a comprehensive understanding of socio-technical issues, and be flexible enough to allow further refinement or additional perspectives (facets) to be integrated into the model with the minimum of effort.

We believe that our focus on security risk management and the domain knowledge captured in our modelling can be usefully applied to the management of collation interoperability in military settings.

4 Model Development

As part of the D3C project we have modelled many areas that contribute to the broad notion of dependability and focused on the more specific areas are required for the management of security risks in order to dynamic balance between information sharing and IA.

4.1 Technical Approach

Studies performed in the first year of the project formulated foci for technology development necessary for such a system. To this end our first pass of ontology development was based on the tool concepts we had developed as part our studies. Figure 3 represents these foci as a simple control loop, involving planning, monitoring and decision support processes.

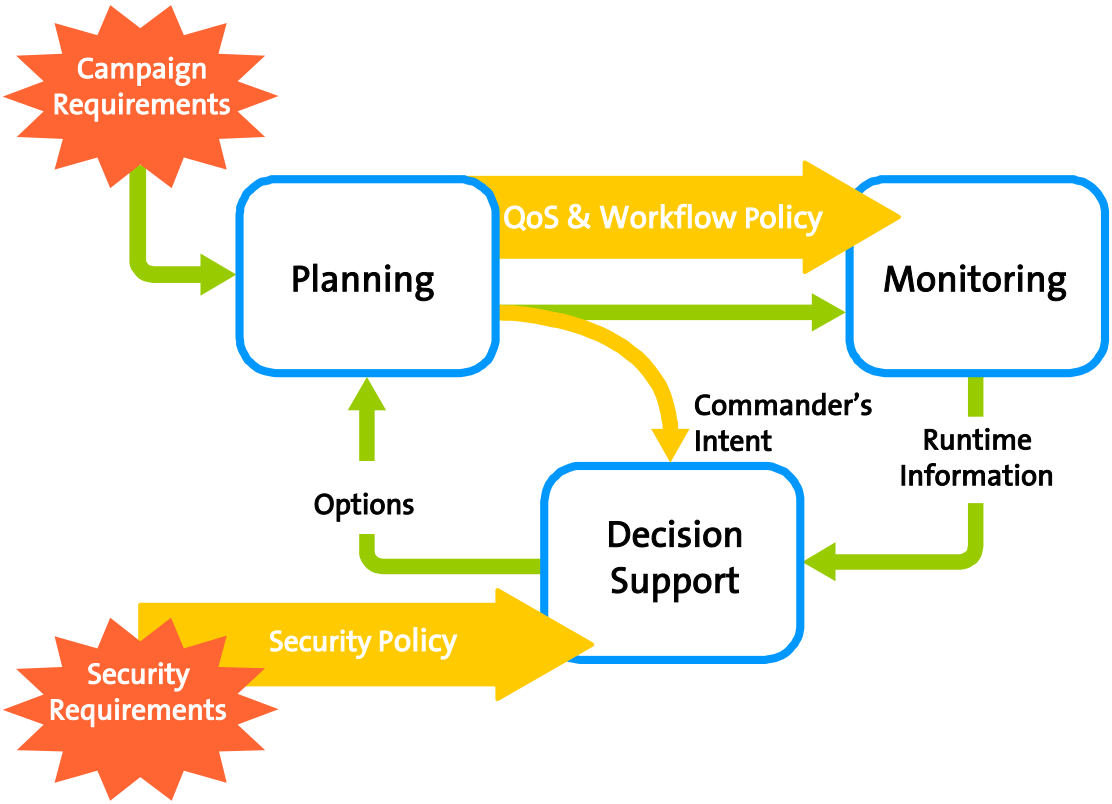

Figure 3: D3C's foci for technology development

Each focus is supported by tooling. We plan to refine I-X tooling [25] for the planning process, and KaOS [26] and Ponder [27] policy engines will form the basis of the monitoring process. From our analysis of the military need, we feel that the Decision Support Tool (DST) offers the greatest potential to move the state of the art forward. Through the DST the D3C project has the potential to greatly improve the understanding of security risk afforded to commanders in the field. This is achieved by pulling more knowledge through from accreditation into the deployment and operational phases, in formalised, consistent models and dedicated tooling.

The DST provides the interface for project engineers, accreditors and system users to enter information about the dependability of the system into the knowledge base. Figure 4 shows the set of editors which comprise the DST, these are:

- **DBSy editor** – describe security boundaries and information sharing requirements providing the basis for our IA modelling.
- **Risk Analysis editor** – assess the security risks associated with the system, builds upon the DBSy model and uses a detailed and refined risk analysis process model.

- **Other system modelling editors** – provide alternative descriptions of systems which may be more low level than DBSy
- **Policy editor** – refine policies for system governance and allow the precise coupling of policy on to system IA models and the resulting risk analysis.
- **Trust and dependability editors** – allow both detailed analysis on specific items in the other models and broader statements that can colour the other views generated.

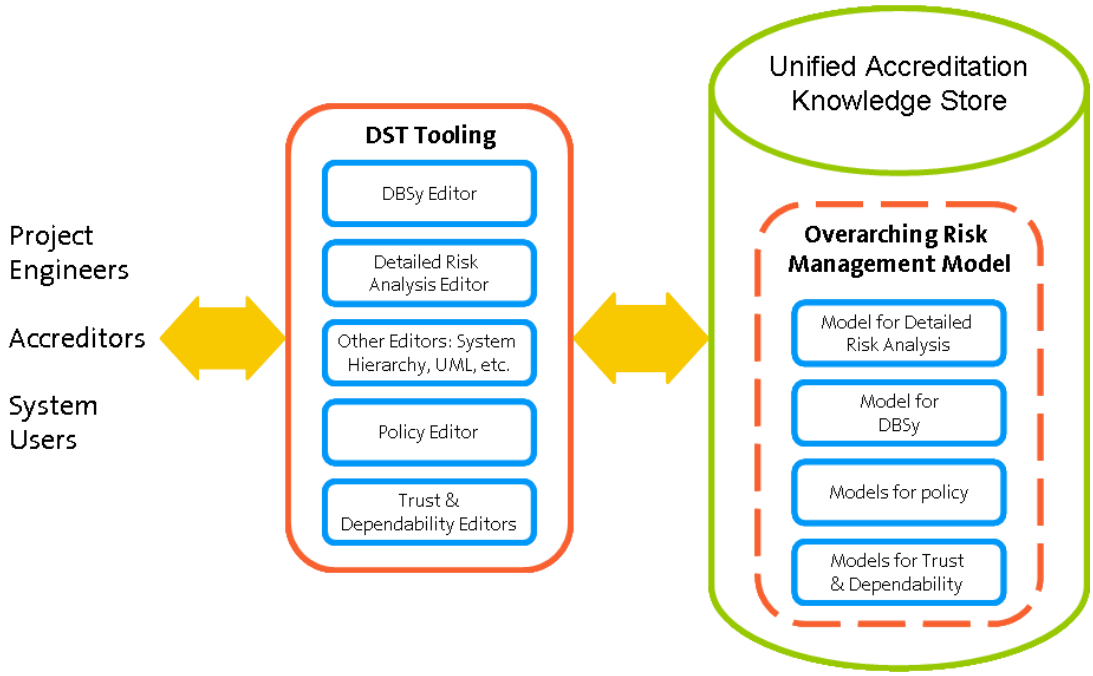

Figure 4: Key models and editors from which the DST is constructed

We undertook surveys for existing technologies that could be built on to reduce the development effort required. The survey identified Protégé [28] from Stanford University, CORAS [29] and the Eclipse tool [30]. Protégé was selected as the ontology development tool and as a means to instantiate models prior to the dedicated editors being developed in order to create the initial straw-man models required for refinement. Eclipse was adopted as the code development tool and had the added benefit of providing an application framework for our editors to reside in and communicate through. CORAS was adopted as a complete, comprehensive framework to approach risk with as it was particularly suited to our mix of trust coalition scenarios.

Taking a model centric approach and using flexible tools such as Protégé and Eclipse also meant that we could rapidly modify the DST's editors in the light of any changes to the underling structure of the models.

4.2 Ontology Development

In line with our socio-technical approach to model development we developed separate models for policy, trust, dependability, DBSy, a detailed risk analysis process and a shared ontology (to provide essential inter domain mappings).

Our models will allow a complete development, accreditation and deployment to be precisely captured and the tooling presents ideal and otherwise unattainable views on these models.

The areas covered by our models are presented in figure 5. Some areas will require refinement for our demonstration programme e.g. in the System Description area we have focused on DBSy, but there are other models, such as those possible thorough more conventional Unified Modelling Language (UML) diagrams.

Although we usually start from a dependability view point, constructs can start from any area modelled and can delegate or refer to other areas. Information classes dedicated to such relationships are added where they are well understood or frequently called upon. Thus a trust statement can use risk analysis as part of its

evidence and a risk statement can use trust as mitigation. The ontology and the tooling are designed to simplify the ontology refinement process and so encourage an evolutionary modelling approach.

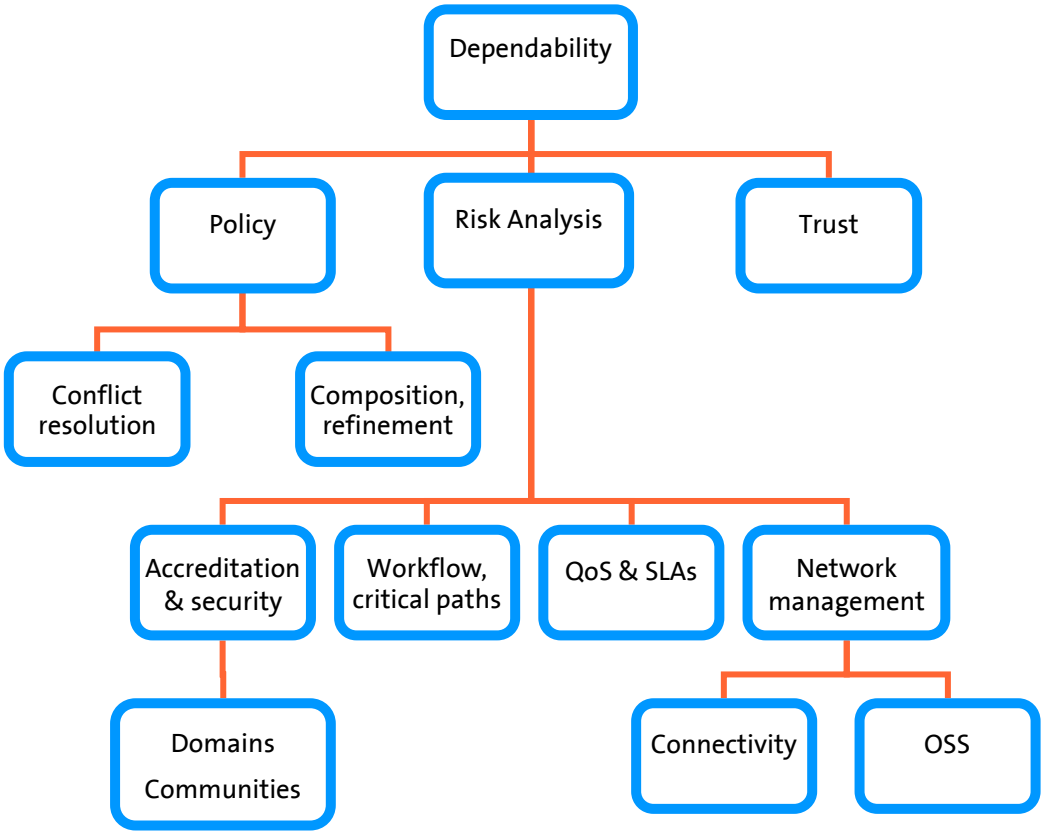

Figure 5: Aspects modelled in D3C ontologies

4.2.1 The core ontology

The core ontology is the key to enabling the tool interactions, and it also enables and plays a vital role as part of a knowledge cycle. Making systems secure and dependable by means of policy is a complex problem, which will require iterative development, as the problem is better understood. The shared ontology will be a means for recoding and re-using that understanding.

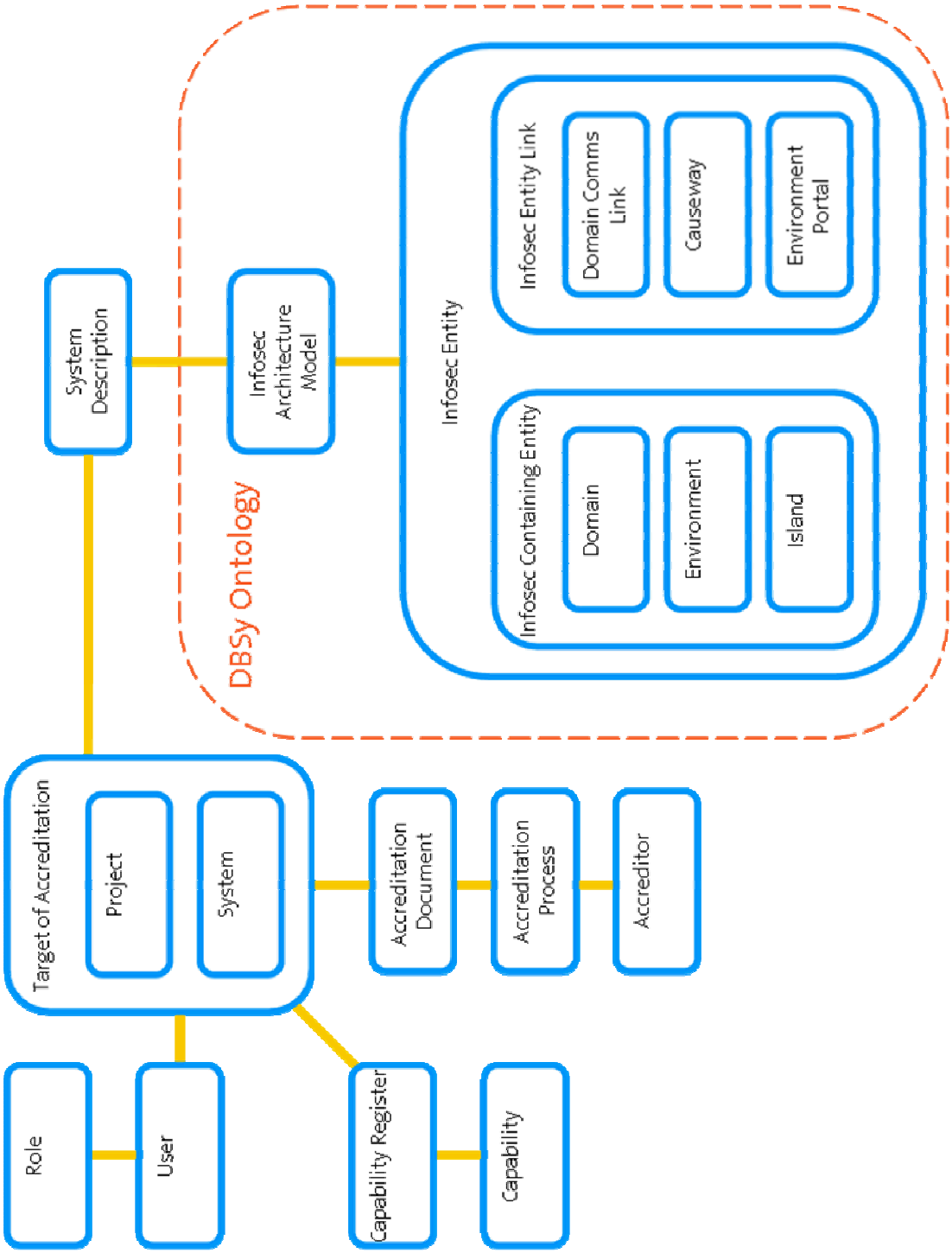

Figure 6: D3C major classes in the 'core' accreditation and DBSy ontology

The informal representation in Figure 6 shows containment is an expression of refinement e.g. a *Project* 'is a' *Target of Accreditation*. The connecting lines represent links, ownership or delegations e.g. a *Capability Register* 'has a' list of *Capabilities* and the *Target of Accreditation* 'has a' *System Description*.

For ease of viewing we have omitted areas of the ontology such as the classes that represent risks and risk registers. A further simplification is that we have omitted each class's parameters; e.g. *InfoSec Entity* has parameters such as *maximum classification* and *minimum security clearance*.

Section 5 has examples of how the core ontology has been used.

Dependability modelling

Figure 7 illustrates some of the key classes from our dependability modelling. It largely follows the comprehensive taxonomy work found in [31]. As with the previous diagram this is an overview omitting all parameters and lower level classes.

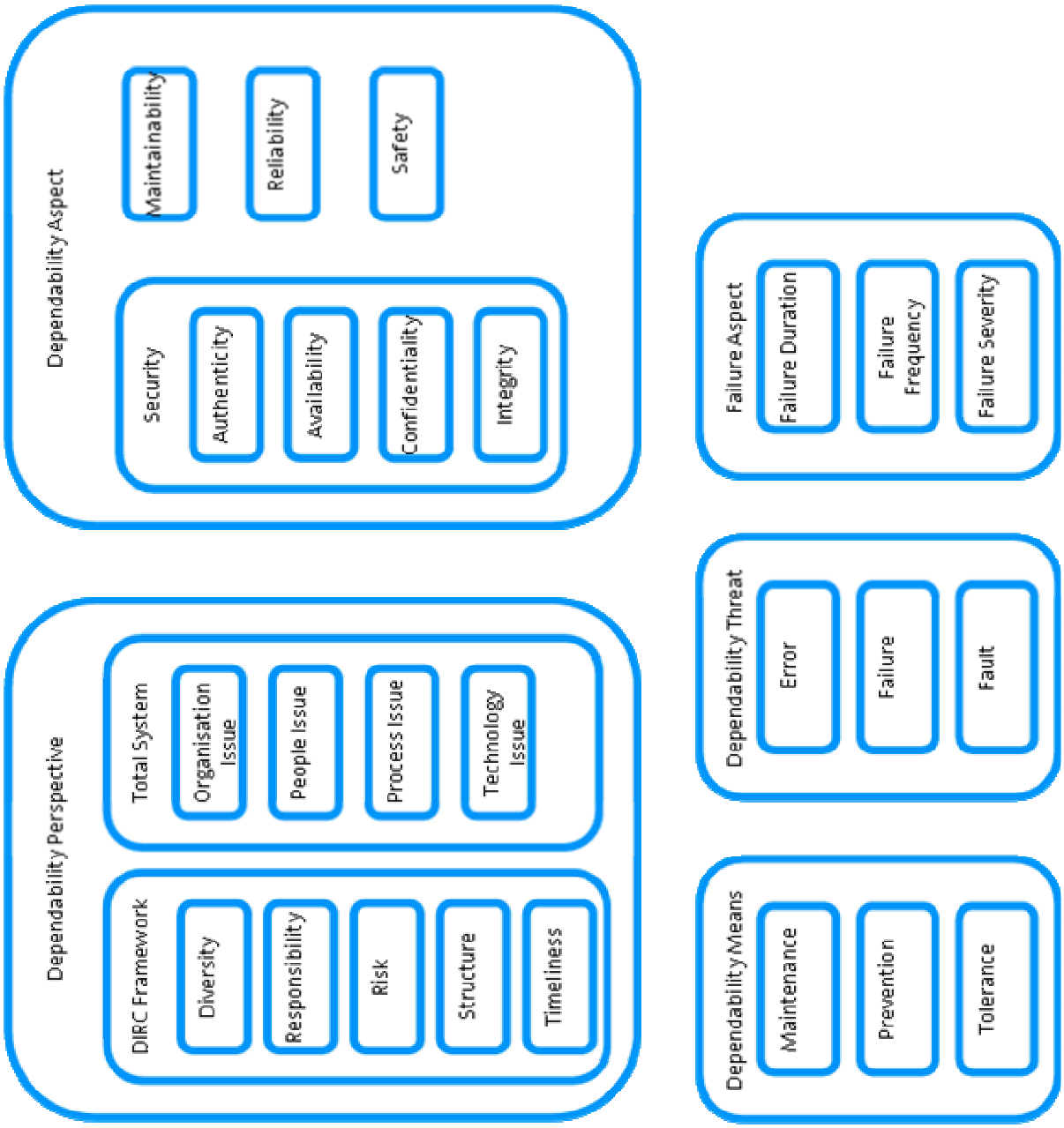

Figure 7: Major classes in the Dependability ontology

Areas omitted from the above diagram include those classes that help build dependability constructs from the classes shown. These allow dependability cases, requirements and status constructs made out of a set of *Dependability Impact* classes with associated classes for representing metrics. Analogous classes can be found in the trust modelling depicted in figure 8.

Dependability Perspective, and its child classes, is being separated to its own *School of Thought* ontology as it has become apparent through a series of expert workshops that each methodology greatly affects the resulting constructs. We hope to improve understanding and interpretation by making explicit which methodologies relate to which constructs.

We are also adding *Interoperability* as a *Dependability Aspect* as this has emerged as a precise meaning that is distinct from *Maintainability* and *Reliability*.

4.3 Trust modelling

Figure 8 shows an overview of the trust modelling afforded in our framework. Some refinement over previous work has been undertaken to help its applicability to SOA and semantic web environments. In figure 8 we have shown an example of some refinement; the notion of '*Understandability'* can now be expressed in terms of *'Accessibility', 'Visibility'* and *'Interpretability'*. This allows us to model a change of trust if a service is simply not available, if we have no direct mapping to its specific ontologies, or if it is intentionally hidden (usually from third parties).

We will also develop a special class of 'Interpretability' that makes explicit its relationship to 'School of Thought'. For example, this could be used in a construct stating that an organisation is 'Trusted' for 'Interpretability' of 'DIRC Framework' 'Dependability Aspects', with annotated links to supporting evidence. This will allow meta-knowledge and reasoning of how well parties contribute to particular aspects of our approach.

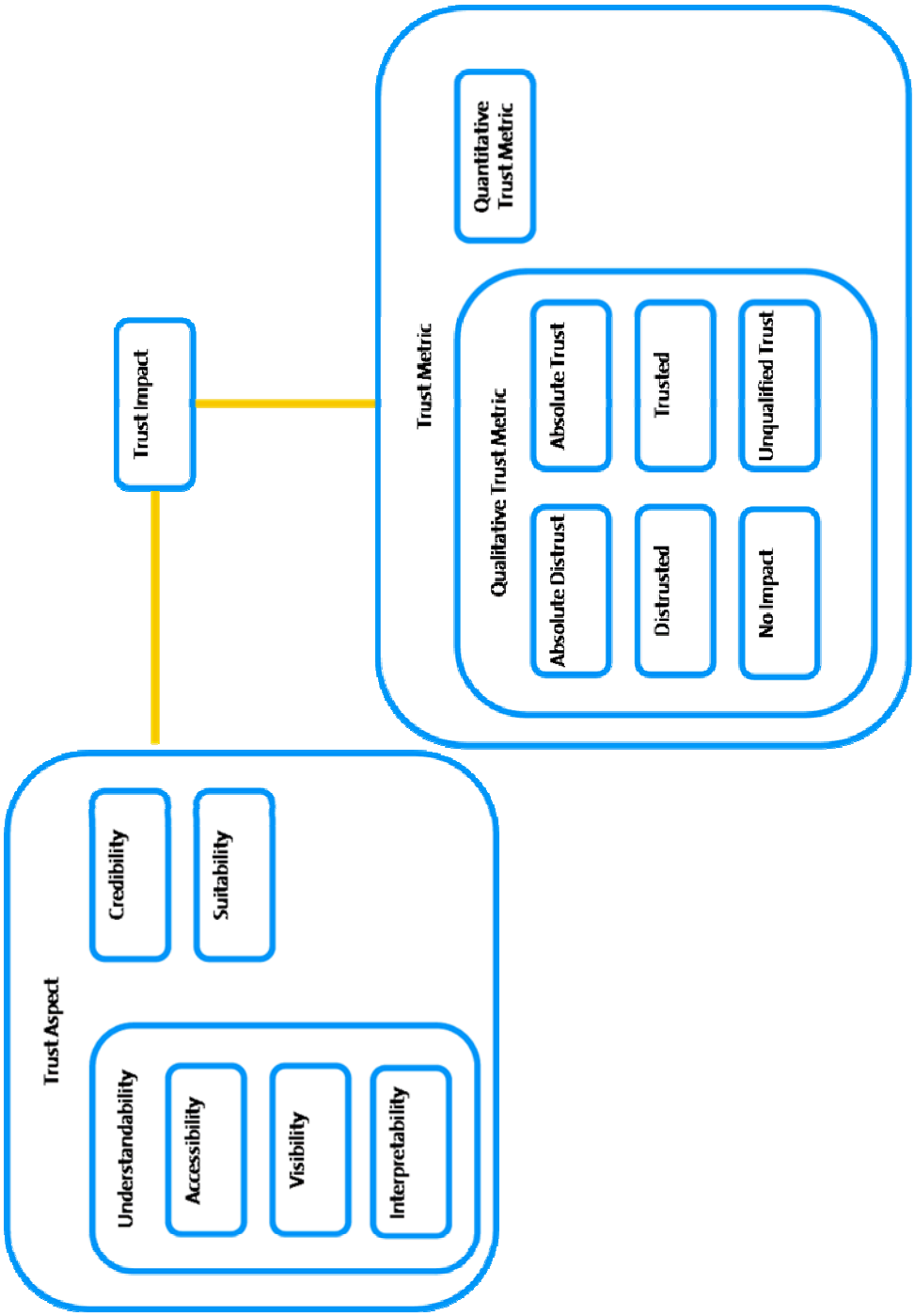

Figure 8: D3C major classes in the Trust ontology

An important aspect across the modelling framework was to allow either qualitative or quantitative judgments to be represented. One of the required parameters of a metric is a 'justification' link. This normally points to another element in the ontology (usually part of a System Description). These kinds of parameters are prevalent in our modelling framework. Optional parameters are also included to allow annotations that can be reasoned upon and provide navigation routes for human operators.

5 Model Exploitation

As we indicated in the introduction to the previous section our initial tooling focus was the DST. Through this tool knowledge is pulled through different human roles and viewpoints with automation to support validation and some specific analysis assistance. In this section we describe how the modelling framework developed has been used to facilitate our DST tooling.

Ultimately this modelling framework will also be able to contribute to automated systems where behaviour can be bounded and deemed as acceptable to accreditors, pushing the envelope for the extent of dynamism and automation in military CIS. Figure 9 provides an overview of some ways that modelling can contribute to the communication and negotiation of security requirements and their risk management.

	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

Figure 9: Human-machine interaction table for D3C Tooling

5.1 System governance through Policies

Considered in its simplest terms, policy control is an attempt to dictate system behaviour through a set of rules. Given the significance of the Word Wide Web Consortium (W3C) Web Services Architecture (WSA) [32] to SOA and semantic web research, we adopted its policy model. However the WSA policy model lacks the ability to express how and why policies contributed to system dependability, so D3C has focused its policy modelling in this area. We believe that the governance of a system through polices that are precisely coupled to our DBSy and Risk Analysis models holds great potential to the future management of military systems. The idea is to allow traceability from the underlying security requirements, through their accreditation, to a particular deployment and how the residual risks are being mitigated.

In the D3C project, policies can be linked to entities to any part of the ontology framework (see section 4.2 and figure 5). Such links define relationships that can incorporate security goals, risk mitigation, trust and dependability. D3C allows Risk Analysis to **a)** be related to DBSy and then **b)** *define* policies. So finally policy can be seen to *embody* the Risk Analysis. The D3C demonstration programme will show the importance of this coupling of information and the benefit of closing the gap of system security governance (figure 10). A motivation for this is to allow broader security issues to be monitored than is currently possible. Using the complete tool set all the issues, concerns, options and judgements can be made available to decision makers when security problems arise further along the system life cycle, as a deployment is being made or as a mission unfolds for example. There is no work we are aware of that attempts the coupling of broad security requirements, risk management and policy definitions; the norm for policy based control is to focus on access control.

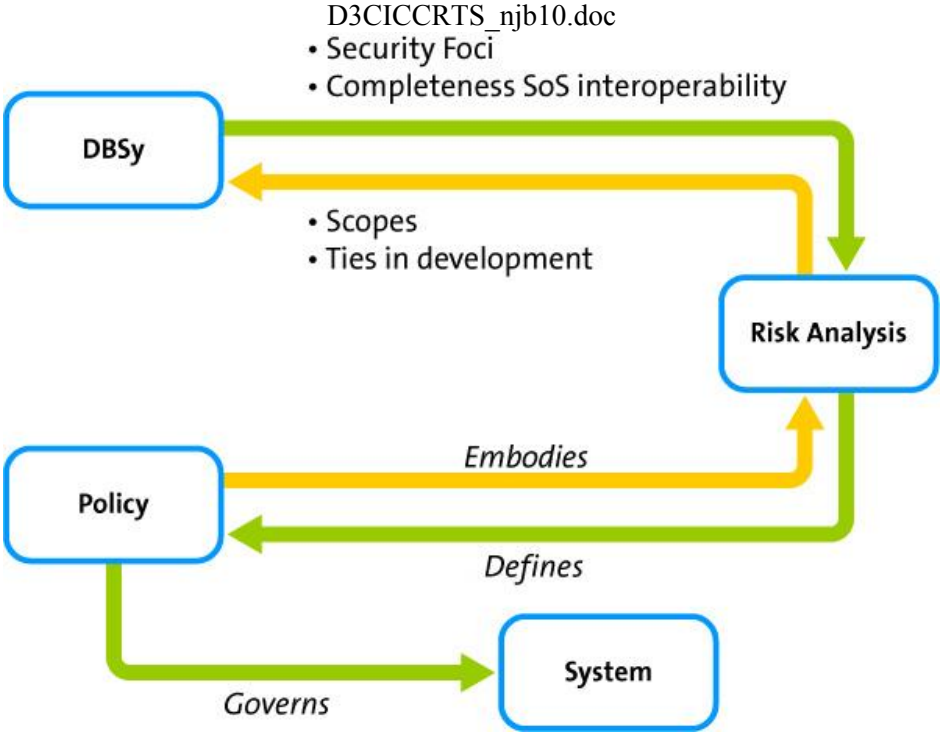

Figure 10: embodying policy with security risk analysis for system governance

By precise coupling of the concerns and justifications of all the roles involved in bringing a system into use through policy statements, there is the potential to present these back to system users when problems are detected by a monitoring capability. We are investigating the use of option 'templates' and building QoS statements that uniquely include broad security requirements.

With our research partners we are exploring the modelling of many types of policy and their relevance to military systems. Of particular interest are policies covering the suitability of security mechanisms in dynamic contexts, and that respond to changes in the operational environment. An important theme that has arisen is the auditable tracing from any current policy envelope to its accredited security policy set and the associated risk analysis.

5.2 DBSy editor Tool

The DBSy editor provides the DST with a capability to develop and navigate complex security models. The diagrams are stored in the knowledge base, making this the first DBSy semantic model. Using the current DBSy nomenclature, models can be developed to capture security boundaries, security requirements and information sharing requirements for a system. These systems can incorporate elements from other such system models, and can be composed to make up 'Systems-of-Systems'.

The editor also provides multiple alternative views on the model, including hierarchical and ownership perspectives, as well as filters which colour the model elements according to their properties, e.g. elements can be highlighted which have violated the validation rules, or elements can be coloured according to the maximum data classification that they are permitted to handle.

Use of this editor can greatly increase the efficiency of knowledge capture during the accreditation process, and the reduction in effort required also allows a fuller treatment to be performed on most systems. Even without the benefits afforded by the use of the underlying semantic model, this tool is proving its use with DBSy modellers who enjoy the speed with which diagrams can be updated and shared. To encourage its acceptance, we have also developed functionality to create and complete some of the DBSy documentation, where tables in a template document are automatically updated with the details from the model.

A key benefit of the DBSy editor allows the revisiting of accreditation during deployment, and commanders can be made aware of the security risks engendered as a result of operational changes.

5.3 Risk Analysis and Compromise Path Analysis Diagram

The Risk Analysis/Compromise Path Diagram Editor provides the DST with a capability to develop, navigate and automatically analyse the risks pertaining to the underlying security model.

The Risk Assessment Tool is based upon the CORAS methodology and framework [29] which is a multinational EU funded project aimed at creating *"tool-supported methodology for model-based risk analysis of security critical systems"*. The version of the CORAS framework we used was 2.0b1 and further work has been done by the CORAS team since then. The current release is 2.1b1 and represents significant work towards tighter integration of UML with the CORAS tooling itself.

5.3.1 D3C's Breadth of Applicability Facilitating Interoperability

The CORAS methodology is very rich and detailed, and our tooling fully encompasses this approach with additional refinements of a core subset of the whole process. These refinements include a more iterative approach to a Risk Assessment and extending the methodology to make use of the DBSy modelling we have developed (see 5.2). By allowing iterative use of the tooling we enable an assessor to jump to earlier parts of the CORAS process at any time and facilitate re-accreditation at runtime This allows an assessor great flexibility to use the relevant parts of the Risk Assessment process for different Risk Assessments and easily scales to encompass large or small projects.

Extending the CORAS framework to use the DBSy methodology was done through the use of a specially designed DBSy ontology (see 5.2) which was then incorporated into the Risk Assessment tooling. This allows us to link the Risk Assessment to semantically rich DBSy models that are able to fully express the Infrastructure (physical) and Business (logical) architectures of the systems being assessed and the separation requirements placed upon them. These DBSy models then define the initial structure for the Risk Assessment, clearly identifying the required physical and logical boundaries and communication links between system entities upon which the security requirements, risks and mitigations are focused.

As our tool uses a general, security focused, Risk Assessment approach there are no hidden assumptions about possible targets of Risk Assessment and it can be applied just as simply to MOD projects/organisations as well as to corporate systems, public bodies like hospitals or civil government departments, NGOs and even full scale coalitions, including the full range of partners, actors and risk types that this encompasses.

At present DBSy modelling is used almost exclusively on systems within the MOD domain. However in coalition situations MOD systems will have to interoperate with systems from many other parties including allied military systems, Other Government Departments (ODG) and NGOs of both home and allied nations. The underlying risk assessment framework, and the DBSy modelling, is fully applicable to any of these types of systems enabling a uniform approach to assessing security risks in coalitions and other 'mixed mode' systems.

With our Risk Assessment tooling project developers, designers and accreditors are able to record their decisions and concerns from the very beginning of a project, and this information is then stored in a knowledge base. As a result decisions and their justifications taken across all stages of the project are available later on in a system's life cycle. This helps those deploying or using a system to make fully informed and risk managed decisions by presenting the relevant information to them in an easily accessible manner which allows 'drilling down' through the details present.

As the methodology underlying the DST has such broad applicability and it provides valuable methods to express and clarify the scope of a Risk Assessment being carried out, it allows interoperability issues between projects and inter-project dependencies to be more clearly defined and explored than is currently possible. Furthermore, the provision of a common modelling language to express the goals, requirements and restrictions of projects greatly improves their interoperability.

5.3.2 D3C's Depth of Refinement Facilitating Interoperability

The level of detail afforded by the CORAS framework and our Risk Assessment tooling allows continual traceable refinement of any element of a risk assessment including risks, systems, treatments and justifications. Additionally the DBSy modelling tool allows infinite refinement of a system through a simple

interface which we are able to fully utilise with the Risk Assessment editor. The CORAS framework itself is able to capture a large volume of information, including details about the system(s) being assessed, the restrictions the assessment has to work within and the differing goals and desires of the various stakeholders. The tooling we have developed presents a core of required information to the assessor whilst allowing them full access to the rest of the information gathering power of the CORAS framework.

By integrating the hierarchical DBSy approach and ontology into the Risk Assessment tooling we are able to define, at many levels of detail, the initial structure for the Risk Assessment, clearly identifying the physical and logical boundaries and communication links between system entities upon which the security requirements, risks and mitigations are focused. This makes very simple the processes of: assessing security risks, and determining threats, vulnerabilities, security requirements and risk mitigations. As all of the information within the Risk Assessment is readily accessible through the editor or ontology the identification of the justifications for the creation and placement of the risks, security requirements etc. is easily located and presented to a user thus passing on the underlying reasoning for a decision and enhancing the user's understanding of the concerns of the risk assessors.

To further aid both assessors and end users the Risk Assessment tooling, in line with and building upon the CORAS framework, allows the creation and attachment of UML diagrams to various parts of the Risk Assessment. The modelling allows for different elements of the risk assessment to be represented in a clear and unambiguous manner and enables clear expression of concerns, arguments and justifications for many parts of the assessment. This enables project developers, designers and accreditors to clearly state their intentions and concerns throughout the system development process and captures these within the Risk Assessment enabling them to be examined at a later date. Furthermore, due to the model based nature of the Risk Assessment tooling users are able to communicate directly through the model in a semi-formalised way reducing ambiguity and potential confusion.

5.3.3 Automation of Risk Assessment & Reasoning

The underlying data-store for the DST is a Protégé ontology which enables the DST (and other tools) to analyse the information captured during a risk assessment and to perform additional processing upon the stored data. Such additional processing could include using any of the plugins for Protégé or other Knowledge Management tools that can use the Ontology in an OWL or RDF format. This ensures that the knowledge captured by the DST and the Risk Assessment is usable by as wide a range of tools and users as possible. It would also be possible to reuse information from previously completed risk assessments in one that is currently being done. This reuse could include the justifications and reasoning for making a particular decision or could simply be copying the use of a particular risk or treatment.

Currently the tooling automates the process of Compromise Path Analysis. This is done by calculating all the possible compromise paths for a given Attack Group and Focus of Interest. Automation could be further developed to provide automated Risk Assessment of systems at any stage of their life cycle, from identifying simple potential problems with a designer's initial model to identifying likely risks and their 'best' treatments whenever a model is changed. Such automation would allow a 'Commander in the field' to make changes to the DBSy model of their system with the tooling providing feedback about the changes in security risks and requirements that result from the change.

Even greater automation, as well as greater user usability, would be achieved through the inclusion of templates to represent default sets of risks, treatments, justifications etc. With the use of such templates it is possible to create a skeleton of a Risk Assessment for a system given nothing more that a DBSy model potentially allowing new systems to be quickly evaluated for levels of potential risk if connected to an already accredited system.

Furthermore, such automation could enable systems assessed with the DST to enter into an automatic negotiation about the requirements that would enable communication between two nodes, potentially allowing the systems to automatically configure themselves in a secure manner which allows them to communicate with new systems on the fly, supporting a fully operational dynamic SOA/SOS architecture. Conversely, if such a negotiation results in a failure to agree, a list of unsatisfied requirements can be generated allowing system engineers to see exactly what would need to be done to enable communication between the systems and to assess if this was possible and desirable.

6 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 could improve the management of interoperability. We would warmly welcome any discussion with researchers in related fields on this topic.

Lessons learnt so far on the D3C project include:

- A social-technical perspective provides a productive direction to provide impact on military CIS.
- Underpinning technology development with scenario development, practitioners' and experts' workshops provide invaluable insight.
- The act of developing ontologies with practitioners and researchers helps define the notions more precisely for those communities, and identifies areas for further research and any false assumptions very effectively.
- Using an ontology development tool such as Protégé greatly enhances the experience and outcomes of these workshops.
- Ontology development is a continuing process as it must adapt to changes in the outside world if it is to remain salient.
- Modelling conducted in order to pull complex knowledge thorough various human perspectives can be automatically validated and reasoned upon.
- Taking a model centric view of development greatly eases the development and refinement of tools that strongly rely on knowledge representation.
- The development and refinement of tooling is further enhanced when implemented in a language that allows introspection/reflection such as Sun Systems' Java as many aspects can be made to automatically adjust to changes in the underlying modelling framework and ontologies.
- 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.

7 References

1. Hughes, K., *Domain Based Security: Enabling Security at the Level of Applications and Business Processes.* QinetiQ/KI/TIM/CP021906, 2003.
2. Prof. Shadbolt, N., *AI expert calls for e-defence for the UK.* Electronics and Computer Science (ECS), 2005.
3. Alberts, D. S. and R.E. Hayes, *Power to the Edge: Command and Control in the Information Age*. 2003: Command and Control Research Program Publications.
4. Board, Command and Battlespace Management, *Joint Service Publication 777 - Network Enabled Capability.* 2004.
5. Defense, Department of. *Network Centric Warfare*. Available from: http://www.defenselink.mil/nii/NCW/.
6. Rathmell, R. A. *A Coalition Force Scenario 'Binni – Gateway To The Golden Bowl Of Africa'*. in *International Workshop on Knowledge-Based Planning for Coalition Forces*. 1999. Edinburgh, Scotland.
7. (AWG), C4ISR Interoperability Architectures Working Group, *Levels of Information Systems Interoperability (LISI)*. 1998, Department of Defense: Washington D.C.
8. *NATO Interoperability Directive (AC322-SC/2-WG/4 WP (2003)0015-REV2)*.

9. (CREST), US Center for Research and Education on Strategy and Technology, *Coalition military operations – the way ahead through cooperability.* Report of a French-German-UK-US working group, 2000.

10. Clark, T. and R. Jones. *Organisational Interoperability Maturity Model for C2*. in *Command and Control Research and Technology Symposium*. 1999. United States Naval War College, Newport, RI.

11. Fewell, S. and T. Clark. *Organisational Interoperability: Evaluation and Further Development of the OIM Model*. in *8th International Command and Control Research and Technology Symposium (ICCRTS)*. 2003. Washington D.C.

12. Stewart, K., et al., *Non – technical Interoperability in Multinational Forces*, in *9th International Command and Control Research and Technology Symposium – The Power of Information Age Concepts and Technologies*. 2004: Copenhagen.

13. Schade, U. *Towards the edge and beyond: The role of interoperability.* in *10th International Command and Control Research and Technology Symposium (DoD ICCRTS)*. 2005. Virginia.

14. Tolk, A. and J.A. Muguira. *The Levels of Conceptual Interoperability Model*. in *Fall Simulation Interoperability Workshop*. 2003. Orlando, Florida.

15. Codner, M., *Hanging Together: Interoperability within the Alliance and with Coalition Partners in an Era of Technological Innovation*, in *NATO Research Fellowship Final Report*. 1999.

16. Morris, E., et al., *System of Systems Interoperability (SOSI): Final Report*, in *TECHNICAL REPORT CMU/SEI-2004-TR-004 ESC-TR-2004-004*. 2004, Carnegie Mellon Software Engineering Institute: Pittsburgh.

17. Wikipedia. *Socio-Technical Systems*. 2005 Available from: http://en.wikipedia.org/wiki/Socio-technical_systems.

18. Emery, F. E. and E. L. Trist, *Socio-Technical Systems.* In Management Sciences Models and Techniques, 1960. **2**.

19. Trist, E. L., *The Evolution of Socio-Technical Systems.* Occasional Paper No. 2, 1981.

20. Trist, E. L., *A Socio-Technical Critique of Scientific Management.* The Social Engagement of Social Science: A Tavistock Anthology, 1993.

21. Dillon, A., *Group Dynamics Meets Cognition: Combining Socio-Technical Concepts and Usability Engineering in the Design of Information Systems.* The New Socio Tech: Graffiti on the Long Wall, 2000: p. 119-126.

22. Sommerville, I., *Software Engineering*. 7th ed. 2005, Harlow: Pearson Education / Addison-Wesley.

23. Ure, J. and G. Jaegersberg, *Invisible Architecture: The Benefits of Aligning People, Processes and Technology: Case Studies for System Designers and Managers*. 2005, Swindon: British Computer Society.

24. Dobson, G., R. Lock, and I. Sommerville, *QoSOnt: A QoS Ontology for Service-Centric Systems.* EuroMicro, 2005.

25. *I-X: Technology for Intelligent Systems*. Available from: http://www.aiai.ed.ac.uk/project/ix/.

26. (IHMC), Institute for Human and Machine Cognition. *KaOS Policy and Domain Services*. Available from: http://www.ihmc.us/research/projects/KAoS/.

27. Policy Research Group, Imperial College. *Ponder: A Policy Language for Distributed Systems Management*. Available from: http://www-dse.doc.ic.ac.uk/Research/policies/ponder.shtml.

28. *The Protégé Ontology Editor and Knowledge Acquisition System*. Available from: http://protege.stanford.edu/.

29. *CORAS Project Home Page*. Available from: http://coras.sourceforge.net/.

30. *The Eclipse OpenSource Community*. Available from: http://www.eclipse.org/.

31. Avizienis, Algirdas, et al., *Basic Concepts and Taxonomy of Dependable and Secure Computing.* IEEE Transactions on Dependable and Secure Computing, 2004. **1**(1): p. 11-33.

32. Booth, D. and et al., *Web Services Architecture*. 2004, W3C Working Group.