

Structural Concepts for Trust, Contract and Security Management for a Virtual Chemical Engineering Organisation

Panayiotis Periorellis¹, Christopher J. W. Townson² and Philip English³

¹School of Computing Science, Claremont Tower 8th floor,
University of Newcastle Upon Tyne, NE1 3RU
panayiotis.periorellis@ncl.ac.uk

²Department of Management Science, The Management School,
Lancaster University, LA1 4YX
c.townson@lancaster.ac.uk

³Department of Chemical Engineering and Process Materials,
Merz Court, University of Newcastle Upon Tyne, NE1 3RU
p.j.english@ncl.ac.uk

Abstract

The paper reports on ongoing research into the development of a management system to co-ordinate a set of activities of a virtual organisation for the production of chemicals. The paper reports on the authors' experience in considering a real virtual organisation and raises issues of co-ordinating atomic activities that span across organisational boundaries and deals with systems that possess a high degree of autonomy and dynamicity. The focus here is on determining the requirements in terms of the co-ordination of parallel activities, trust and security issues such as access control, validation of resources and identities, formalisation, risk analysis and finally fault tolerance.

Keywords: Trust Requirements, Spheres of Control, Software Application Structuring, Software Architecture, Dependability for Virtual Organisations, Chemical Engineering

Introduction

In organisations of vital importance is trust, which is essential for them to work effectively or at all. Means of facilitating trust are the formalisation of procedures such as manuals, specifications, or contracts. Other ways are in personal interactions which give confidence to interested stakeholders that activities will be undertaken satisfactorily. In the virtual organisation context, an important difference is that these personal interactions are either severely curtailed, are not possible, or even discouraged. This increases perceived risk for the stakeholders as their trust in their partners reduces.

To mitigate against this, a virtual organisation will require a computer-based management system which will give stakeholders confidence that activities carried out by others are occurring in a manner that they are comfortable with – here this will be referred to as a trust management system. In order to fulfil this requirement, this system will need to have a number of interlocking components. These are a formal language for policy expression, verification of user credentials against policies, contract expression and validation, risk assessment and generation, and maintenance of reputation values for all participants.

Although procedures and bureaucracy enhance trust, they are also time consuming and inconvenient. In the virtual context these are manifested as login requirements, password usage and other protocols. Dependability is largely considered a trade-off between security and convenience. The inconvenience of bureaucratic mechanisms in real life is experienced through tasks such as the time and human resources needed to undertake specified tasks; in the virtual world this will manifest as additional processing capacity, resources, etc.

A lack of bureaucratic mechanisms in virtual organisations can result in problems such as unauthorised access, loss of information, deceit, etc. The legal framework, in current English law (Walden, 2004), hardly supports the notion of a virtual organisation which encompasses issues such as virtual agreements (contracts) as well as the ones mentioned earlier. Therefore there is a need to provide mechanisms which will bridge this gap¹. In computing literature there are two notions of trust: that of access control and resource validation, and that which encompasses the wider business sense which deals with risk analysis.

There has been a significant amount of research examining risk analysis aspects which relate to trust (e.g. Josang and Presti, 2004); this paper, however, focuses on structural issues (McKnight and Chervany, 2002) and includes access control, authentication, and policy making. The view taken is that fault tolerant structuring will promote trust and hence dependability, while at the same time minimising the risk of security breaches.

To illustrate these facets of trust management in a virtual organisation, an example from the chemical engineering industry has been chosen. The business challenges that this industry faces in the United Kingdom includes the outsourcing of the majority of chemical production to low cost countries, such as China and India. To mitigate against these challenges a number of responses have been identified (Cavalla, 2003). In terms of market forces, Lien and Perris (1996) include shorter product lifecycles; the production of speciality products (e.g. food and pharmaceutical); improved and consistent quality; more ‘agile’ and efficient performance of multi-product processes. They also state that reduced lead times, compression of the design lifecycle – ‘time to market’ (Beßling *et al*, 1997), and the integration of legislation and standards into the development process will play an important role in increasing the competitiveness of the UK chemical engineering industry.

¹ Although it is outside the scope of the current paper, it must be remembered that organisations may not trust the data that they receive even if it can be electronically guaranteed to be correctly passed by others. For example, there may be feelings of unease as to its accuracy and that it may be falsified. Brown and Lockett (2004) discuss the importance of trusted third parties which may go some way in tackling this crucial issue.

Crucially, Lein and Perris (1996) have identified that more flexible and responsive manufacture, distribution and supply, is also critical in improving the chances of the UK chemical engineering industry being able to compete. They state that virtual organisations ('extended enterprises') are likely to play an important role in responding to the threat posed by low-cost overseas competition.

The paper reports on work which is part of the GOLD project (Grid-based Information Models to Support the Rapid Innovation of New High Value-Added Chemicals). GOLD is concerned with highly dynamic organisations whose formation and sole purpose is the satisfaction of a market opportunity. Consequently the virtual organisation is disbanded or reformulated to pursue other market opportunities. The GOLD project aims to deliver the enabling technology to support the formation, operation and successful dissolution of virtual organisations. Middleware technologies are to be developed to address issues such as trust, security and information management for virtual collaboration between companies.

Virtual Organisations and GOLD

From the above, it may be seen that GOLD differs from most of the so-called virtual organisations referenced within the computing literature which usually describe organisations that are built over time and last for a number of years (Nayak *et al*, 2001), CISCO systems being a good example. Of particular concern are organisational entities that can be rapidly integrated to exploit a market opportunity. To enable this, a set of standards will need to be defined which all participating organisational entities will adhere to. The result of such an exercise is not a virtual organisation as such, but in effect a virtual market of potential collaborations across organisational boundaries. Hence a virtual market is a set of autonomous organisational entities that conform to a set of pre-determined rules that guide the integration process. These rules may deal with low level protocols, security issues such as access control, description of interfaces as well as high level policies such as ownership of service, data, etc. Dynamic virtual organisations are represented in the following diagram. The cones (nodes) represent the market, that is, a set of organisational entities that conform to market rules. The lines represent the flow of information between organisational entities. Each topology reflects a particular a market opportunity being exploited.

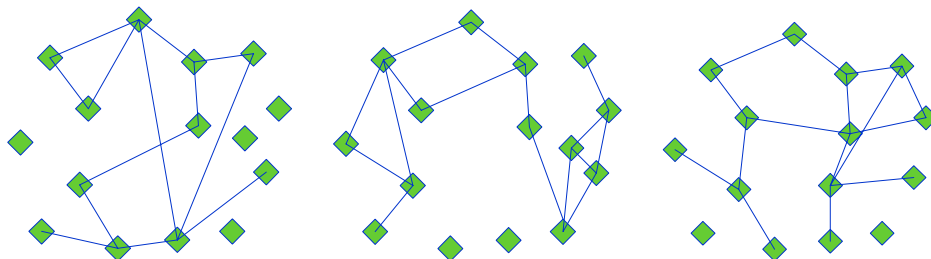


Figure 1. Virtual Markets and Topologies of Virtual Organisations within the Virtual Market.

From the above, a virtual organisation could be defined as a manifestation of a network of enterprises within a virtual market for the sole purpose of exploiting a market opportunity as described by the virtual organisation's topology.

GOLD Lifecycle

In the chemical engineering sector, the production of a chemical is realised via the outsourcing of a number of activities that span from gathering data about a particular chemical and safety analysis through to production. For that purpose several vendors may be involved. GOLD will provide the platform through which this type of collaboration can be achieved. The majority of activities are outsourced to various companies all of which can communicate with each other using GOLD. From a computer science perspective, issues which need to be addressed are the crossing of organisational boundaries, carrying out contract management, providing access and indirect access to certain resources, assessing the associated risk at all times, coordinating atomic activities while at all times remaining dependable. The following figure shows three activities of GOLD.

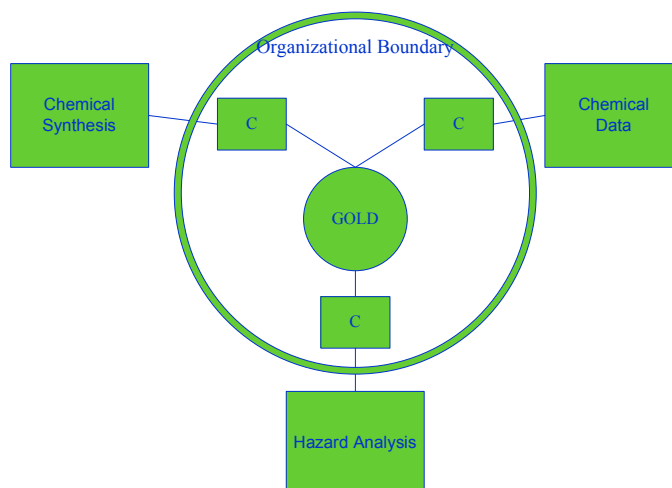


Figure 2. Part of the GOLD lifecycle for the production of a chemical.

Figure 2 above illustrates part of the life cycle of GOLD. Responsibility for composing the whole service resides with GOLD, which in this case is the production of a specific chemical. Some of the activities may be carried out in parallel. For that purpose distributed controllers are used that handle specific activities (indicated in Figure 2 as c). The diagram shows GOLD distributed controllers which are software modules which handle specific pre-determined activities. Before the concept of distributed controllers is explained, we take a look at general dependability needs requirements that gave rise to their requirements will be examined.

Dependability Issues

The nature of the system to be built will be largely deterministic since it is bound by contractual arrangements. That is not to say however, that the state space is either small or manageable. From a dependability point of view, a number of issues need to be dealt with such as fault analysis, trust management and risk analysis. Although fault analysis to a larger extent, and trust management to a lesser, are issues that have

been addressed in computer science literature, risk assessment and its relation to exception handling is somewhat novel. In this paper the implication is that rather than simply using distributed exception handling techniques to handle transactions, distributed risk assessment tools will be used that can optimise the parallelisation of activities (within the chemical engineering life cycle) and determine the cost/benefit and consequence of all transactional activity (regardless of its output) with each of the organisational units.

Here, both fault tolerance techniques will be used such as forward error recovery (FER) and backward error recovery (BER). In cases, for example, of a breach of contract, it cannot be assumed that a failure or return to the previous non-erroneous state will occur. Forward recovery is required to ensure that the system is constantly moving towards its goal state (i.e. production of the chemical) by applying correction techniques to the erroneous state. In the case of a breach of contract scenario, especially if it is late in the development of the chemical, ideally the error should be corrected, for example, by using a new service provider. In cases, however, of transacting with a particular service provider, it will be necessary to apply backward recovery in order to resume a transaction that reached the erroneous state.

Exception handling is the mechanism by which FER and BER may be implemented and is an important aspect of the system (Garcia and Rubira-Calsavara, 2001). Exception handling in general contains a number of hidden properties that can both hinder or enhance the performance of the system depending on its structure and deployment of handlers. In the case here, it is mostly dealing with specific activities some of which are co-dependant in terms of input/output, while others may be parallelised. An example of the former in the later stages of the chemical engineering lifecycle would be the legal requirement of a full HAZOP (HAZard and OPerability study) having to be completed before plant operation/chemical production is begun. An example of the latter being work associated with the scale-up of a proposed chemical synthetic route being run in a more parallelised manner with synthetic route development. Hence, scalability of a potential route may be considered to be practically in parallel with the traditional criteria for chemical route selection leading to a more rapid solution and a time saving for chemical development lifecycle.

The optimisation of processes in this manner is what hopefully will give a competitive advantage to those using GOLD. Parallelisation of activities requires the propagation of exceptions, which in turn implies distributed exception handling capability for the system. Here the issue of distributed exception handling and risk analysis (associated with each particular distributed parallel activity) will be addressed by providing different application layers, each of which possesses different degrees of authority. Propagating an exception to a higher layer implies that decisions have to be taken by the application layer of the higher authority. Propagation of exceptions however, may imply ‘flooding’² especially as the number of parallel activities increases. Therefore the concept of spheres of control (Davies, 1978) will be used to enhance the dependability approach with the concept of error confinement. This implies that handlers are dedicated to address specific faults raised by specific parts of the system, while faults that cannot be dealt within the sphere are propagated to a higher layer.

² ‘Flooding’ in this context means that too many exceptions are created for the exception handlers to cope with.

Arguably trust and trust management are somewhat ill defined in the computing literature. This paper does not seek to clarify these definitions, suffice to say that the distinction is made between the concept of trust as a ‘calculated risk one willingly accepts’ or a ‘reliance placed by a on b to deliver’, and trust management which encompasses authorisation issues and access control. The concept of reputation is also being explored as part of the GOLD project. The reputation of the service provider is important in a competitive market such as chemical production. Mechanisms are being explored where activities carried out by various organisational entities have a weighting by which GOLD can use to make decisions regarding service composition. The majority of the concepts regarding structure are envisaged via the controllers shown previously Figure 1. They allow a conceptualisation of distributed autonomous decision making while at the same time providing error confinement and structured exception handling. Controllers are ‘aware’ of the grouping of activities, trust management issues, risk management issues and exception handling. In order to facilitate the distributed production of chemicals, the technology encompasses all the theoretical issues that have been discussed earlier. The following diagram examines their structure.

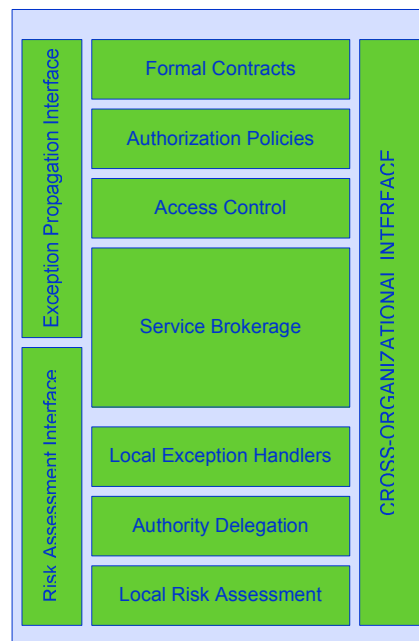


Figure 3. Controller Structure and basic components.

The cross-organisational interface serves the purpose of linking the organisational units with the controllers. Across the interface, information is passed such as the contract definition, the authorisation policies, the user’s credentials as well as the details of the service. The service brokerage component maintains details of interface specifications of each organisational unit with the potential of carrying out a particular activity. The exception handler may be thought of as a set of managers which deal with unusual (but predictable) events raised by the activity that the exception handler monitors. They assist the activity in resolving problems locally and support the concept of error confinement. The access control, contract management and the risk assessment modules are now examined in more detail.

Access Control

Traditionally, trust has been engendered between organisations with the help of legal agreements. These formal and explicit contracts can be read by (solicitors of) all parties and form important legal agreements of what can be expected (at least to a degree) by all parties. In the virtual context, Walden (2004) notes that data is even more transient than in traditional arrangements. Thus the use of technology allows arguments to be made that technical malfunction, interference and fabrication have occurred – hence the importance of mitigating against this as described previously. In the United States of America, electronic signatures now have the same legal status as those which are written. This has reduced the liability of electronic transactions. In a multi-stage product lifecycle such as that in the chemical industry, the virtual organisation concept would mean that different enterprises would, as in the traditional context, have to use electronic signatures (or other means) on proposals, contracts and other documents. Furthermore, these enterprises need, in some form, to be ‘aware’ of each other. Awareness mechanisms may be considered to be a resolution to the issue of latent forms of co-operation which may take place between the nodal points of the virtual organisation. Here awareness is defined as the comprehension of activities and goals. The converse of awareness is privacy. Issues relating to the privacy of data are crucial to trust in a virtual organisation. A number of trust management proposals tackle problems of anonymity or lack of adequate data to verify one’s identity by requesting additional information without enough attention on the legal aspects of privacy. Privacy is a policy-level issue and relates to the use of data in the context of consent established by the data owner. Mechanisms for privacy of elements in a virtual organisation are necessary in order to prevent monitoring of sensitive activities and confidential data. The balance between awareness and privacy may well be very delicate as in a highly dynamic virtual organisation partners may also simultaneously be competitors elsewhere. To achieve this balance at the level of the controller, the following schema may be used.

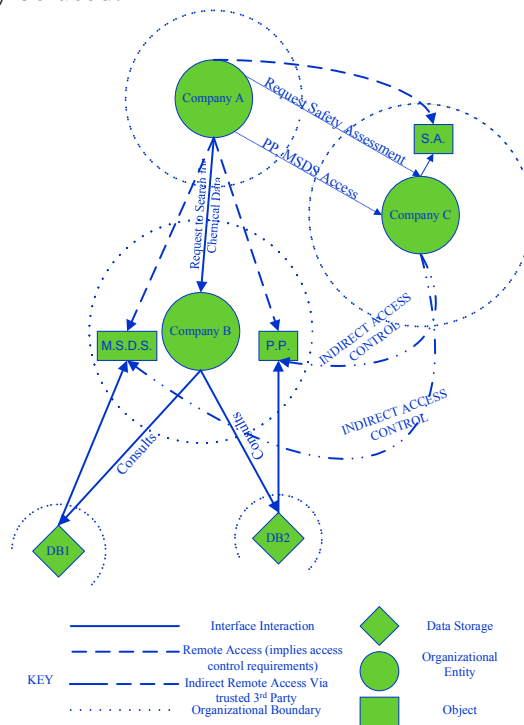


Figure 4. Access Control Requirements.

Figure 4 illustrates a very small part of a virtual organisation's activities for the production of a chemical. An activity, for example such as 'collect data for chemical', requires the usage or interrogation of a number of sources (e.g. databases, web content, and documents). The associated controller will ensure that the activity will be carried out according to time, quality and quantity specifications set by GOLD. At the same time, controllers are aware of the critical nature of those activities and their impact on the overall aim of GOLD (i.e. production of chemical). As such, they are able to carry out exception handling related to each particular activity as well as risk assessment. Additionally, activity specific security and trust requirements such as access control, contract management are also handled here. The concept of distributed activity specific controllers allows support of security and dependability, while at the same time delegating responsibilities from the main authority (which is GOLD) to different application layers.

In Figure 4, Company A has a requirement to produce a safety assessment (SA) for the production of a chemical production where there are a number of autonomous organisational entities shown within organisational boundaries. Firstly, Company A requests details about the chemical from company B. Company B consults a number of databases (which may be remote or in-house), and uses the data returned to produce Material Safety Data Sheets (MSDS) and Physical Properties documents (PP) which are maintained locally. Company B grants access to company A to view the documents. Company A then uses these documents to produce a safety assessment. The assessment is actually carried out by company C. Access to MSDS and PP is required by company C in order to comply. Company A uses its access rights to company B to grant access to company C to view the documents. Company C produces the safety assessment report and grants view access to company A. Company A uses this report to make a decision whether or not to produce the chemical. The example demonstrates the importance of a number of issues and requirements such as:

- Access control over remote locations, crossing organisational boundaries.
- Indirect access control via a third trusted party.
- Dependability assessment access on resources via three or more parties.
- General dependability concerns regarding responsibilities on quality assessment or reliability of objects that are accessed via apparently transparent domains.

Therefore there is a need to not only address issues of access on remote objects but also delegation of responsibility and indirect access via a third party. In Figure 4, which is a depiction of a chemical production process, there is a need to provide mechanisms which would allow company B to effectively collaborate with C (access MSDA and PP documents) for the purpose of carrying out the request to provide Company A with data. There a number of dependability issues relating to constructing systems by propagating or delegating responsibilities as mentioned by Armstrong and Paynter (2002) and Armstrong (2003).

Contract management

Contract management is a difficult concept to deal with in the chemical engineering virtual organisation domain. This is because there are a number of pre-existing

contracts with a number of pre-defined terms of reference and clauses, which are used to rapidly outsource part of the life cycle of the development of a chemical (ICHEM, 2003). It is part of the requirements of GOLD to provide an electronic medium through which this rigid and rather standardised approach is supported and enhanced. This issue will be dealt with here using structured exception handling (Romanovsky *et al*, 2003) and verification techniques. Consider the following diagram.

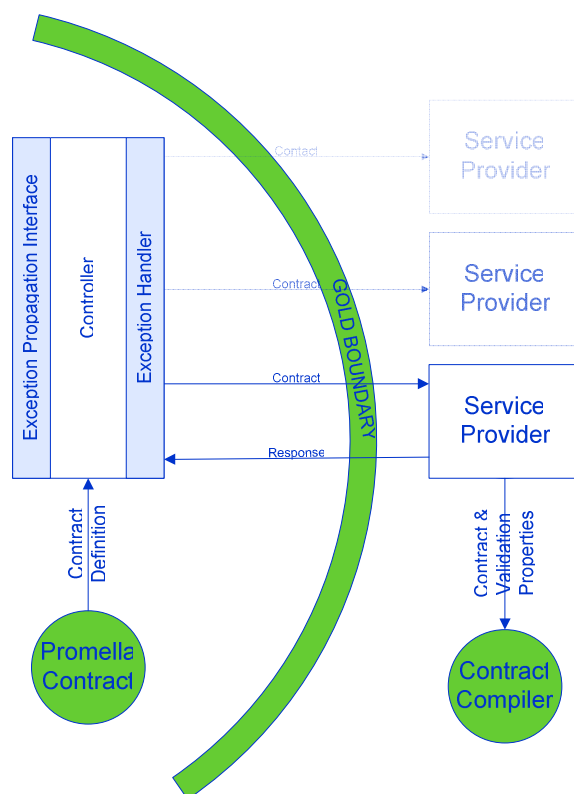


Figure 5. Promela Usage for Contract Validation

As Figure 5 indicates, the Promela programming language (SPIN, 2004) is being used to express pre-defined contracts formally (Molina-Jimenez *et al*, 2003; Solaiman *et al*, 2003). The controllers which act as brokers in this first instance (i.e. the period of time for composing the service from autonomous organisational entities³) will pass the details of the contract (i.e. the Promela definitions) through a pre-existing interface to the potential service provider. It is at the discretion of the service provider to validate the contract definition against certain properties such as deadlocks, reachability and assertion violations. Upon validation by the service provider a response is sent to GOLD to either indicate the provider's commitment to the contract or disagreement. The way this disagreement will be handled is via exception handlers. The handler may, for example, decide to outsource the service to a new service provider and follow the same process (shown faded in figure 5). Additionally if this option is not possible the handler may propagate the exception to a higher authority within GOLD.

³ Autonomous organisational entities are combined to form a service. This service therefore enables the simplification of processes and the virtual organisation will be able to operate with greater efficiency and/or efficacy.

Risk Analysis

The risk assessment component evaluates the progress of the activity based on the exceptions thrown. Additionally, the component has two interfaces for propagating problems to a higher authority. These can be considered as the interfaces of the sphere of control. The exception propagation interface propagates exceptions thrown by the activity and cannot be dealt with locally. For example, if the activity cannot be completed for any reason then the system needs to be informed. Similarly the risk assessment interface propagates assessments of risk evaluation to the higher authority where the overall risk assessment is held. This particular idea deviates from the typical exception handling process (such as that discussed by de Lemos (2003)) in the sense that even if FER or BER are successful, the risk may have increased (due for example, to the time taken for an exception to be dealt with) to the point where the main authority considers terminating the entire process. This is an issue raised by the particular critical nature of the domain to which this is applied and additionally the risk associated with parallelising activities. The way risk is dealt with in the first instance is presented in the following diagram.

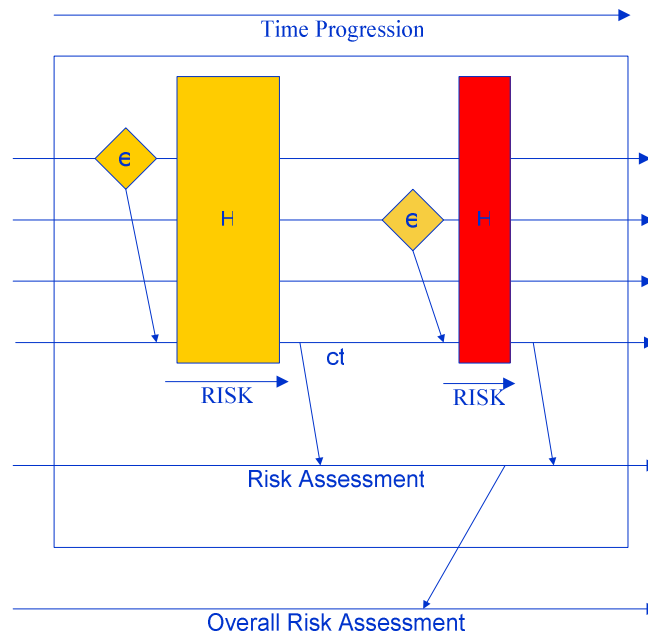


Figure 6. Risk Assessment using spheres of control.

In Figure 6 above, each box denotes a sphere of control inside which several parallel activities take place as indicated by the horizontal lines. When an activity raises an exception e , the controller ct , catches the exception and starts a handler H . The accumulated risk associated with handling the exception is estimated and communicated to the local risk assessment activity. Depending on whether it reaches a critical level (as it has in the second handler) the controller sends the information to the overall risk assessment tool.

Future Work

From what has been discussed in this paper, it can be seen that there are many challenges which will be involved in fulfilling the objectives of the GOLD project.

The high-level conceptualisations described here will require further research in order to yield practical solutions to support a virtual chemical engineering organisation. It will be crucial to know the business/organisational issues surrounding these topics. This will help in the understanding of how (or whether) companies will be willing to participate in a virtual organisation. Appropriate theories will need to be identified which will help to provide insights into these issues. Modelling of business processes will be undertaken to show how a virtual organisation may work. This will then need to be linked to the more technical computer science level shown here. Research will therefore be required to determine how this may be undertaken.

A robust application is being designed using layered exception handling that allows delegation or propagation of responsibility using concepts such as spheres of control and error confinement. This will manifest itself in the form of controllers. The access control model will be designed to handle all requirements of the individual policy makers as well as techniques for the verification and validation of user's credentials. Of particular challenge will be the delegation of responsibility in the form of granting access to an entity to resources via three or more parties. Furthermore, the compilers for Promela contracts using web services and XML schemas will be used.

Conclusion

The paper has presented some requirements and conceptual models for dealing with the general security and trust issues which have arisen when considering a real virtual organisation that deals with chemical development. In an industry where the traditional model of work is outsourcing the idea of virtual organisation where much of the bureaucracy, and therefore time and effort, is eliminated or greatly minimised is almost revolutionary. This however poses a great deal of effort and responsibility on the actual information systems that manage the formation, operation and dissolution of the virtual organisation. In this paper a number of requirements regarding security and trust have been presented alongside potential conceptual models for dealing with these issues.

Acknowledgements

The authors are supported by the EPSRC GOLD project. We would like to thank Nikos Mihalodimitrakis for his contribution on Access Control.

References

- Armstrong, J. M. and Paynter, S. P. (2002). 'Safe Systems: Construction, Destruction and Deconstruction'. In: Redmill, F. and Anderson, T. (eds.), *Current Issues In Safety Critical Systems*, pp. 63-76, Springer-Verlag, Berlin.
- Armstrong, J. M. (2003). 'Danger: Derrida At Work', *Interdisciplinary Science Reviews*, **28** (2), pp. 83-94, IoM Communications Ltd., Newcastle upon Tyne.
- Beßling, B., Lohe, B., Schoenmakers, H., Scholl, S. and Staatz, H. (1997). 'CAPE in Process Design – Potential and Limitations', *Computers and Chemical Engineering*, **21**, S17-S21.
- Brown, D. H. and Lockett, N. (2004). 'Potential of Critical e-applications for Engaging in e-business: a Provider Perspective', *European Journal of Information Systems*, **13**, 12-34.

- Cavalla, D. (2003). 'The Extended Pharmaceutical Enterprise', *Drug Discovery Today*, **8** (6), 267-274.
- Davies, C.T. (1978). 'Spheres of Control', *IBM Systems Journal*, **17** (2), 179-198.
- de Lemos, R., Gacek, C. and Romanovsky, A. (2003). 'Tolerating Architectural Mismatches'. In: de Lemos, R., Gacek, C. and Romanovsky, A. (eds.), *Architecting Dependable Systems*, (pp. 175-194). Series: Lecture Notes in Computer Science, **2677**, Springer-Verlag, Berlin.
- Garcia, A.F., and Rubira-Calsavara. (2001). 'A Comparative Study of Exception Handling Mechanisms for Building Dependable Object-Oriented Software', *C.M.F., Journal of Systems and Software*, **59** (2), 197-222.
- ICHEM. (2003). *The Burgundy Book - Form of Contract, Target Cost Contract*, Institution of Chemical Engineers.
- Josang, A. and Presti, S. L. (2004). 'Analysing the Relationship between Risk and Trust'. In: Jensen, C., Poslad, S. and Dimtrakos, T. (eds.), *Proceedings of the 2nd International Conference on Trust Management (iTrust)*, Oxford, 29th March 2004, (pp. 135-145). Series: Lecture Notes in Computer Science, **2995**, Springer-Verlag, Berlin.
- Lien, K. and Perris, A. (1996). 'Future Directions for CAPE Research Perceptions of Industrial Needs and Opportunities', *Computers and Chemical Engineering*, **20**, S1551-S21557.
- McKnight, D. H. and Chervany, N. L. (2002). 'What Trust Means in e-commerce Customer Relationships: an Interdisciplinary Conceptual Model', *International Journal of Electronic Commerce*, **6**, 35-53.
- Molina-Jimenez, C., Shrivastava, S.K., Solaiman, E. and Warne, J.P. (2003). 'Contract Representation for Run-time Monitoring and Enforcement'. In: *Proceedings of the 2003 IEEE International Conference on E-Commerce (CEC 2003)*, Newport Beach, California, USA, 24th - 27th June 2003, Chung, J.-Y. and Zhang, L.-J. (eds.), (pp. 103-110). IEEE Computer Society Press.
- Nayak, N., Chao, T., Li, J., Mihaeli, J., Das, R., Derebail, A., Soo Hoo, J. (2001). 'Role of Technology in Enabling Dynamic Virtual Enterprises'. In: *Proceedings of International Workshop on Open Enterprise Solutions: Systems, Experiences, and Organizations*, September 14-15, Rome, Italy.
- Solaiman, E., Molina-Jimenez, C. and Shrivastava, S. (2003). 'Model Checking Correctness Properties of Electronic Contracts'. In: *Proceedings of the International conference on Service Oriented Computing (ICSOC03)*, Trento, Italy, December 2003, (pp. 303-318). Series: Lecture Notes in Computer Science, **2910**, Springer-Verlag, Berlin.
- Romanovsky, A., Periorellis, P. and Zorzo, A.F. (2003). 'Structuring Integrated Web Applications for Fault Tolerance'. In: *Proceedings of the 6th International Symposium on Autonomous Decentralised Systems (ISADS 2003)*, Pisa, Italy, April 2003, (pp. 99-106), IEEE Computer Society Press.
- SPIN. (2004). Spin manual web page. <http://spinroot.com/spin/Man/Manual.html>
- Walden, I. (2004). 'Addressing the Data Problem: The Legal Framework Governing Forensics in an Online Environment'. In: Jensen, C., Poslad, S. and Dimtrakos, T. (eds.), *Proceedings of the 2nd International Conference on Trust Management (iTrust)*, Oxford, 29th March 2004, (pp. 1-15). Series: Lecture Notes in Computer Science, **2995**, Springer-Verlag, Berlin.