Current capabilities, requirements and a proposed strategy for interdependency analysis in the UK

Robin Bloomfield[1,2] , Nick Chozos[2], Kizito Salako[1]

[1] Centre for Software Reliability, City University London. 10, Northampton Square, College Building, EC1V 0HB, London, UK.
{reb, kizito}@csr.city.ac.uk
[2].Adelard LLP, 10, Northampton Square, College Building, EC1V 0HB, London, UK.
nc@adelard.com

Abstract. The UK government recently commissioned a research study to identify the state-of-the-art in Critical Infrastructure modelling and analysis, and the government/industry requirements for such tools and services. This study (Cetifs) concluded with a strategy aiming to bridge the gaps between the capabilities and requirements, which would establish interdependency analysis as a commercially viable service in the near future. This paper presents the findings of this study that was carried out by CSR, City University London, Adelard LLP, a safety/security consultancy and Cranfield University, defense academy of the UK.

Keywords: Critical Infrastructures, Interdependency modelling and analysis, R&D strategy

1 Introduction

The UK Centre for the Protection of National Infrastructure (CPNI), the Technology Strategy Board (TSB) and the Engineering and Physical Sciences Research Council (EPSRC) commissioned a feasibility study to identify the state-of-the-art in Critical Infrastructure (CI) interdependency modelling and analysis and to develop a strategy for research and practice, aiming to bridge the gaps between existing capabilities and Government/industry requirements.

The study, carried out by the Centre for Software Reliability of City University, London, Cranfield University, Defense Academy of the United Kingdom and Adelard LLP resulted in two publically available reports:

- The 'main' report [1], which presents the overview of capabilities, requirements and the proposed strategy.
- A secondary report [2], which is an introductory research review in the areas of modeling, analysis and visualization of infrastructure interdependencies.

This paper will briefly present the study, discuss some of its findings, and conclude with the proposed strategy.

2 Background: The Cetifs study

The Cetifs (CPNI, EPSRC, TSB Interdependency analysis Feasibility Study) methodology comprised the following activities:

1. Analysis of two recent major UK multi-infrastructure disasters: The Buncefield explosion [4] and the 2007 floods [5].
2. Consultations with a wide a range of Critical National Infrastructure (CNI) stakeholders (government, industry and academia)
3. A review of research specific to modeling and analysis of dependencies in CIs (in a separate report, [2]).
4. A questionnaire survey based on the three previous activities distributed to utility companies IT and security departments

The Buncefield explosion

The explosion that took place at the oil storage depot located in Buncefield in December 2005 has been characterized as the biggest explosion in peacetime Europe. The explosion affected the operation of multiple infrastructures (energy distribution, transportation, information infrastructure, finance, health as well as the environment). This incident is of particular importance as it unveiled some important issues with regard to information infrastructures (II).

We mainly focused our analysis on an IT company/data centre named Northgate Information Solutions, which was severely affected by the explosion. The servers that were at these premises hosted patient records and admission/discharge for a number of hospitals in the area, a North London payroll scheme of approximately £1.4 billion, and systems/data for several local authorities [4] among others.

The 2007 floods

The floods that struck much of the country during June and July 2007 were extreme, affecting hundreds of thousands of people in England and Wales. It was the most serious inland flood since 1947 [5]. 13 people lost their lives, approximately 48,000 households and nearly 7,300 businesses were flooded and billions of pounds of damage were claimed. In Yorkshire and Humberside, the Fire and Rescue Service launched the "biggest rescue effort in peacetime Britain".

The floods affected multiple infrastructures, such as water and food supply, power, telecommunications and transportation, as well as agriculture and tourism. Many businesses also suffered flooded sales premises, together with damage to stock and equipment.

Incident analysis conclusions

The analysis of these incidents helped us to understand some of the challenges that infrastructure owners and the government are facing. We found that there are several

issues which, although they are known, they are not well understood. These served as a basis for our consultations and were the following:

Geographical dependencies are, to a certain extent, known, as the identification of physical proximity of assets is straightforward, especially when we consider an area surrounding a plant or within a flood-vulnerable area. Nonetheless, there were several surprises in these events (*e.g*., during the floods, several critical services had to be shut down for precaution in case the flood reached them but there was uncertainty as to whether that was actually needed or not). There are also more complex and indirect consequences (*e.g.*, the effect the Buncefield explosion had on the adjacent business park and the data centre in particular was also deemed as a surprise).

Competition for resources. This challenge arises during an incident and can also lead to interdependencies or further cascade effects. Capacity and bandwidth of resources are known to infrastructure owners; however, during crises they may be reached very quickly, and in unusual ways. Competition for resources can also manifest when an asset that provides a resource is lost (*e.g.* a power station), where other dependent nodes will have to find alternative suppliers.

Long term effects. In some cases, major incidents can involve significant long term loses to infrastructure and economy by complex cascade paths. One typical aspect of this is the effect a disaster can have on tourism. In the Pitt review there was an extended discussion on the role of media following the floods and the long-term effect on tourism and the economy of affected areas. Although there are a number of studies in macro-economic impact of infrastructure failures, the long term effects of such disasters and how they can be controlled are aspects that are not well understood and require more detailed analysis, considering various parameters such as the role of media.

We also concluded that there is a *lack of empirical data* to support in-depth analyses that will help us understand interdependencies better. This is due to the comparative rarity of events, and the difficulty in attaining data from multiple organizations, with many incidents going unreported or kept as anecdotes within one infrastructure. As part of this study and continuing work with TNO [7] we are analyzing the implications of their large infrastructure incident database [1].

2.3 Consultations and questionnaire survey

The consultations formed the biggest part of this study; in particular, we carried out semi-structured interviews with:

- Parts of the UK government that are concerned with the prevention of and response to major CNI disruptions, resulting either from attack or natural disaster. These consultations helped us formulate the context of the study and the requirements that Interdependency Analysis (IA) services would have to satisfy.
- Private companies and research institutions that develop tools or use them to offer services that can assist in the identification of interdependency vulnerabilities. These stakeholders provided us the understanding of what the state-of-the-art is, and what capabilities can be offered currently.

Before discussing the requirements and capabilities, we ought to present the different perspectives that stakeholders have as these perspectives pose different sets of requirements and interests in IA. These perspectives have been organized around the concept of resilience, as it provides a useful framework within which to consider different stakeholder approaches, requirements and responsibilities for CI services.

Perspectives on CNI resilience

Interdependencies are often discussed as a source of threat to systems. Indeed this can be the case and in particular unforeseen interdependencies can be a source of surprise and uncertainty in our ability to understand risks and system behavior. However interdependency is also central to providing tolerance to attack and failure, a means for adaptation and overall resilience.

The loss of system capacity due to an incident can be seen as an indication of how resilient a system can be. This viewpoint is shared by the US Department for Homeland Security (DHS) and UK Resilience. This resilience perspective is shown in Figure 1 below.

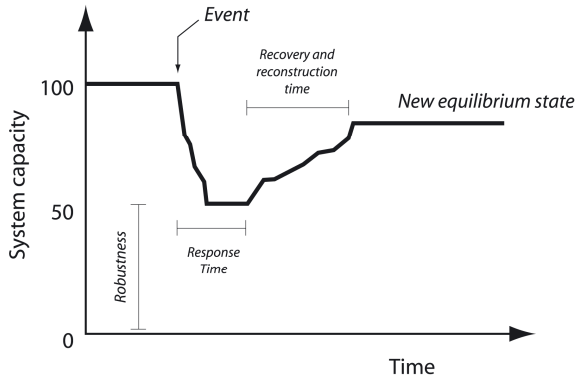

Fig. 1. Resilience

However in [6] the emphasis is on the ability of a system to adapt and respond to changes in the environment. In a recent report for the Defense Science and Technology Laboratory (DSTL) [3] produced by CSR, City University London, two types of resilience were distinguished:

- *Type 1: Resilience to design basis threats*. This could be expressed in the usual terms of availability, robustness, etc.;
- *Type 2: Resilience to beyond design basis threats*. This might be split into those known threats that are considered incredible or ignored for some reason and other threats that are unknowns.

Some policies consider an "all hazards" approach that addresses both malicious and accidental attacks on systems. In addition, the notion of *dependability*, or dependability and security, as an umbrella term is useful to capture the need to

address all attributes (safety, security, availability etc.) rather than just a single attribute.

The overall service level view is summarized in Table 1 below:

Table 1. Phases of resilience

Phase	Action to increase resilience
Preparation and learning	Reduce frequency of events by early warning and upstream measures. Provide early warning, operator support. Learning from experience (major incidents, minor mishaps, near misses), training.
Initial loss	Increased robustness by - Network design addressing topology, redundancy, diversity. - Classification of critical nodes and suitable hardening. - Understanding of events and scenarios
Detection	Communication between services. Variety of forecasting approaches. Detection of compromises.
Decision	Situational awareness. Planning and training (scenarios) and use of synthetic environments.
Recovery	Resource deployment; dependent assets identified - Awareness state of other networks. - Communication and co-ordination.

The different stakeholders all had an interest in resilience but had very different emphases. Broadly speaking these concerned the scope of their responsibilities, whether it was:

- *All hazards approach*: all hazards are considered, including both natural disasters and malicious attacks;
- *Security and vulnerability focus*: identification of security critical assets and consideration of vulnerabilities/threats to them;
- *Natural hazard focus:* only considers events such as floods/earthquakes and their effect on CNI;

And also the overall purpose of their analyses e.g.

- *Identification* of vulnerabilities (dependencies) in stable system state;
- *Incident response*, i.e., control of the incident and evacuation and coordination of emergency services;
- *Long-term effects and recovery* e.g., environmental, financial.

We can use the resilience-dependability framework to capture the different perspectives of stakeholders. For example, those of CPNI and the UK Home Office Civil Contingency Secretariat (CCS) are shown in the table below.

Table 2. CPNI and CCS perspectives

Framework component	Stakeholder: CPNI	Stakeholder: CCS

What services are addressed?	All within scope of NI suitably prioritized.	All
Which dependability attributes are concerned?	Classic security attributes – confidentiality, integrity, availability.	Emphasis on availability.
What range of hazards/ threats?	Security related only.	Natural hazards in terms of initiation. Advice from CPNI on security. All hazards in decision and recovery phases.
Which resilience phase?	Emphasis on prevention and preparation and learning phase. Advice to CCS during incidents.	National risk assessment deals with long term losses. Emphasis on recovery and incident response.
What services are addressed?	All within scope of NI suitably prioritized.	All

A security evaluation could then be seen as evaluation of resilience for certain threats (e.g. malicious ones) and for certain attributes (confidentiality, integrity, availability). The evaluation of the security part of resilience would then address the different stages of Table 2.

In this study we were particularly interested in (inter-) dependencies, and so we can use the framework to assess what dependability attributes, what resilience phase and what threat scope is of concern and being addressed by particular modelling and analysis approaches.

Questionnaire survey

We further explored these issues with a small questionnaire survey that was targeted at utility companies IT and security managers.

From the responses we have received, we found that utility companies address the challenges of infrastructure interdependencies by ensuring close relationships with suppliers and vendors. They believe that close relationships can assist in understanding the various risks associated with their providers' failure and their overall level of resilience. Risks are monitored through internal risk review groups, and company boards oversee the results. Also in some cases utilities hold industry forums to exchange information, or engage in regular review meetings. Exercises involving suppliers have also been carried out. In some cases, alternative providers have already been sourced as part of contingency planning.

However, the protective measures to be taken depend on the nature of the risk or vulnerability and on the particular department. Overall, utility companies focus on improving resilience by having business continuity planning, frequent risk assessment, back up systems (especially for IT), as well as security technologies.

Although infrastructure dependencies are considered in risk assessment, this is mostly done in more traditional ways, without tool support. In one case, it was suggested that mapping software was used, although just once, for examining proximity of functions to cable routes. In addition, none of the respondents were aware of any technical documentation, research or conferences in infrastructure interdependency, something which perhaps suggests the presence of a gap between research and practice.

Most responders suggested they had experienced either minor or major disruptions due to failure of other infrastructure providers.

The questionnaire also probed whether there was scope for some form of IA as a distinct service. There was no clear consensus from respondents; some believed it could be, and some suggested they would be interested if it was part of a wider, risk assessment service. The issues of trust and confidentiality were raised as serious obstacles.

2.4 Research review

The models and simulations developed to support infrastructure modelling and simulation are diverse and complementary. There are multiple ways in which these models are related and there is no single taxonomy or classification that suits all purposes.

In the review we focus on the results of the models to provide a basis for describing relationships between them. The classification of modelling activities from this perspective, applied in particular to models, tools and methodologies is provided in [2]. This includes:

- *Abstraction level and model boundaries:* Questions such as "how much of the real world should be modelled?" constrain modelling methodology and the applicability of modelling results. A continuum of possibilities exists ranging from high-fidelity (very detailed) simulations to mid-range and low-fidelity models;
- *Technique and underlying theory:* (Inter)dependency analysis of complex systems has been recognized as an inherently interdisciplinary activity. There exists a wealth of experience and knowledge relevant for (inter)dependency modelling. This column in the table below gives information about established formalisms, theory and techniques used in building and analyzing the models;
- *Model applicability:* The type of problems where the model can provide useful support is indicated in this column and the extent of tool support.

The incident analysis, the consultations and the questionnaire survey helped us to formulate the requirements, while the research review and again the consultations helped us to evaluate the state-of-the-art, the current capabilities. Capabilities and requirements are discussed in the following two sections.

3 Initial requirements

From our discussions with stakeholders we concluded that:

1. There is recognition that interdependencies are part of wider issues of understanding infrastructure interaction.
2. They are concerned that they lack knowledge of infrastructure interactions.
3. There is sufficient expert judgment, anecdotes and incident analysis to suggest that this lack of knowledge may present a significant risk or a missed opportunity for improving resilience at all stage of the resilience lifecycle.
4. They see many potential advantages in a more sophisticated approach to infrastructure modelling but at present they do not know under what circumstance these uncertainties are significant and so can not justify the required investments.

In discussion with stakeholders we identified requirements across various areas that relate to infrastructure interdependencies. These areas are the following:

- *Inherent infrastructure resilience—scope and overall methodology:* Perspectives here address the level of resilience that is built in to infrastructures and normal operation.
- *Infrastructure analysis and support:* The consultation identified a number of different possible service delivery perspectives.
- *Hazard and vulnerability identification and management:* Perspectives vary on the scope of hazards to be addressed or the approach to the management of systems.
- *Resilience phases:* Potential capabilities and requirements that concern the various phases of resilience.
- *Critical information infrastructures:* A greater focus is given in this study to CII.
- *Dependability of the modelling:* An integral part the development of tools and analytical services is to ensure that they are dependable. There will be a need to trust the results of infrastructure modelling and analysis and possibly integrate information from a variety of trusted and less trusted sources. There will therefore be a variety of confidentiality requirements on the modelling tools and supporting IT infrastructure depending on their application and mode of service delivery. Unless these confidentiality requirements are met the modelling activity could provide a threat.
- *Evidence of costs and potential benefits:* Cost and benefit issues have to do with costs of failure and benefits of IA.

4 Current capabilities

Providers of infrastructure modelling and/or (inter-) dependency analysis are either government-endorsed organizations, or leading private technology solutions providers. Overall, they offer a diverse range of services. Our consultations have aimed at understanding their capabilities and market deployment approaches. These will then be related with, and contrasted to, the initial requirements in section 3.

Figure 2 presents the components that we have considered in this study (see [2] for more detail).

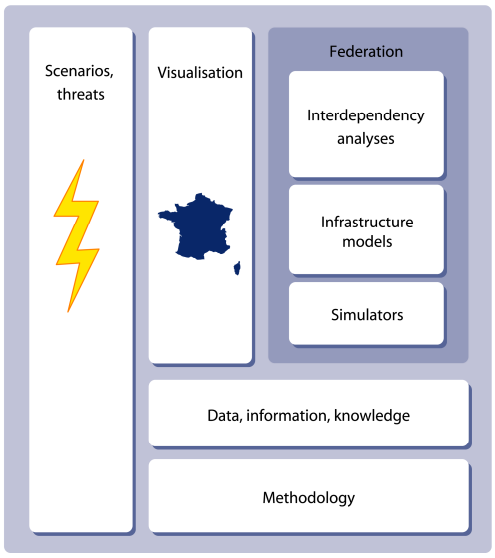

Fig. 2. Modelling components

These components are explained as follows:

Data, information and knowledge. This refers to the data that is fed into the simulation. Data can be either static or live. For instance, simulators are often linked to live weather feeds, GPS and other forms of live data sources. Data acquisition and verification are important challenges as insufficient, incorrect or inaccurate data can result in a misleading analysis.

Federation refers to the integration of several simulations (federates). This is primarily done through achieving interoperability among separately developed simulators. Standardization is required in order to define common elements.

Infrastructure models. Modelling within a single infrastructure or system is a diverse and mature field. Models are fundamental to understanding system behavior, evaluating risks and designing operational strategies.

Interdependency modelling can be considered according to the different perceived layers (e.g. of physical, control and supervisory management) and also in terms of a range of abstractions from high-level services to detailed implementations. For each of these abstractions, there are a wide range of possible modelling approaches and theories that can be deployed, ranging from qualitative models, stochastic activity networks to complexity science style models and high-fidelity simulations. These can be deployed at a varying levels of detail, e.g. to model the detailed implementation topology or to model the service topology and cascading effects.

Methodology. A defined and structured approach can assist in an efficient and effective modelling and analysis. The methodology contains aspects of requirement elicitation, data gathering and analysis, modelling, simulation and the eventual development of conclusions and decision support.

Scenarios and threats. Scenario development considers situations and sequences of events that are of particular concern, in order to identify threats and gain insight of the 'system' behavior under hazardous conditions. In most cases, a 'reasonably' worst case scenario is needed in order to focus planning and mitigation against a threat that has a realistic likelihood of occurring.

Simulators. Simulation is the imitation of some real thing, state of affairs, or process. There are many different types of computer simulation—the common feature they all share is the attempt to generate a sample of representative scenarios for a model in which a complete enumeration of all possible states would be prohibitive or impossible.

Visualization refers to the graphical representation of the modelling and analysis. This can be either on a standalone PC screen, or on large, operating room screens, or over a set of various screen types, sometimes even distributed across various locations. Geographical Information Systems (GIS) are a typical example of visualization. In IA, visualization tends to be layered, with several filtering options to guide decision support and communication.

5 The importance of "intangible" infrastructures

One significant result from our consultations is the importance of "soft" intangible critical infrastructures, e.g. *trust and confidence* within society both in their own right and as an important component that is essential to the functioning of critical services. For instance, trust between individuals, between individuals and organizations and between these and the representative of the state is essential for the delivery of service. This, as with so many of the infrastructures, is often hidden but comes to the fore in times of crisis and recovery from disaster.

Trust is an asset that can be built-up, destroyed, squandered and undermined as with so many other assets and resources. If we are to assess interdependencies we need to take into account these essential yet softer aspects and their relationship to the more tangible aspects. Such assessment should appreciate that these soft aspects are just as much the target of security threats as the more obvious physical and cyber systems. Indeed, it may be that a patient and well read adversary would have a strategy that targets these assets. For example, the financial infrastructure relies very heavily on trust in the banking system for it to function at all. Witness the latest credit crunch, the Northern Rock bank crisis and also public trust in government announcements and the panic buying of petrol because people did not believe assurances about supply. An adversary strategy that relies on people legitimately taking their money out of a bank is far more effective than any physical raid on the bank (unless one wants to get rich). At a micro-level, social engineering attacks that exploit people's willingness to give passwords away can be seen as a form of attack exploiting confidence.

While in the past the soft infrastructure might have been separable from the more technical infrastructures they are clearly related. Trust in the competence of government and authorities is dependent on how well they cope with crises and incidents in both the physical and soft infrastructures. Moreover trust relationships

that citizens have between themselves, organizations, government and agencies are strongly dependent on the information infrastructure: a trend that is likely to increase (see the UK transformational government agenda [8]).

Assets such as trust and privacy within society are important and can be seen as emergent properties; although they are affected by local aspects of trust they have a complex relationship to localized issues. Trust in organizations and government may exhibit the classic complex systems phenomenon of rapid transitions and "tipping points".

Understanding the role of trust and confidence in the protection of CI to the extent where it can be taken into account in CI modelling is arguably a great challenge. This is an active research area (e.g. [10]) but, most work is focused on the application of trust models for the development of trusted IT networks, e.g. for information sharing, but the wider implications of trust seem to be under investigated currently.

6 A proposed strategy

The final part of the study was a gap analysis between the requirements and capabilities identified (as discussed in sections 3 and 4 respectively) to identify whether further research and development might be required, and if so, what form it should take.

IA needs a sufficiently rich model for the analysis to discover and assess the risks:

- Societal aspects need assessment as they provide possible hidden sources of commonality;
- Modes of operation have to be rich enough. These should include degraded modes of operation as they can amplify risks as levels of redundancy assumed at design time become defeated;
- Non-linearities in failure models (e.g. increased failure rates due to stress from nodes in the same locality) can lead to escalation and cascading effects.

We have identified four main potential capabilities:

- To provide specialized security analysts with a means for the assessment of interactions and interdependencies;
- To provide off-line support for risk assessors both aggregators of risk (as at CCS) and also individual infrastructure owners to evaluate the impact of dependencies and interdependencies;
- To provide off-line support for risk assessors both aggregators of risk and also individual infrastructure owners to evaluate the impact of dependencies and interdependencies during incidents (soft real-time);
- To provide real-time, decision support integrated command and control systems (hard real-time) that takes fully into account the impact of dependencies and interdependencies.

To address the required capabilities and gaps that we have identified the study proposed the following:

Trial state-of-the-art and emerging research. Develop and trial modelling approaches and decision-support tools and methodologies at various levels of detail. The trials would consider both qualitative approaches and off-line, soft real time and

hard real-time infrastructure interactions. The modelling would consider functional, topological and probabilistic approaches. The trial should be sufficiently complex to enable scalability issues to be addressed and consider a number of different infrastructure mixes e.g.:

- Energy distribution (*e.g.* gas, electricity);
- Information infrastructures;
- Soft intangible infrastructures (*e.g.* trust, confidence).

The output of the exercise would be experience with the modelling approaches, assessment of costs/benefits and way forward and provide more clarity in current and future stakeholder requirements.

Real-time environment provide particular challenges and these should be addressed separately. Consider proposed future of decision support systems for key stakeholders and develop more detailed requirements to integrate interdependency approach.

Develop an interoperability approach to infrastructure modelling and analysis (e.g. by use of standards, interoperabilities, published Application Programming Interfaces (APIs)). This should promote both innovation and also a more componentized approach. Interoperability should cover behavioral models, topologies and associated data. Data costs can be significant and interoperability can provide an approach to amortizing data costs across applications.

Provide policy support and evidence base. Provide justification and focus of the programme, emphasizing the benefits and responsibilities for all stakeholders.

Define credible business models taking into account the fact that infrastructure and interdependency modelling has particularly close coupling to policy and to sensitive areas of risk assessment.

Offer knowledge transfer and coordination. Promote the research base and offer connection to practice by enabling interaction (e.g. via knowledge transfer activities), addressing costs of research and methodologies and developing a challenging research agenda.

Within each of these threads both natural hazards and security vulnerabilities need to be considered (e.g. by the emphasis in different scenarios).

7 Conclusion

This paper presented an overview of a study that was carried out by the Centre for Software Reliability of City University, Cranfield University, Defence Academy of the United Kingdom and Adelard LLP.

The study was based on consultations with a wide a range of Critical National Infrastructure (CNI) stakeholders (government, industry and academia) and a review of research specific to modelling, analyzing and overall understanding dependencies in infrastructures [1],[2]. The consultations and the research review identified to potential capabilities that would address current requirements and proposed a strategy aiming at achieving the capabilities that were identified as currently feasible.

Acknowledgements: We would like to thank Phil Nobles from Cranfield University, Defense Academy of the UK who was member of the study consortium. In addition,

we would like to thank the consultees who contributed to our study and namely the UK Civil Contingency Secretariat, the Australian CIPMA, Priority5, BT, BAe systems, Northrop Grumman, SE Validation, the European Commission's Joint Research Centre, DG INFSO Unit F5 'Trust and Security' and Unit A3 'Internet; Network and Information Security', Spearhead Technologies, ESRI UK, as well as the members of the SCADA and Control Systems Information Exchange who participated in our questionnaire survey.

We would also like to thank members of the UK CIIMWG who represent a range of key UK government departments.

The study has been funded by TSB, CPNI and EPSRC under contract NSIP/001/0001 – Feasibility Study on Interdependency Analysis. There has been partial financial support from our institutions and from the EU project IRRIIS (027568).

References

1. Bloomfield R, Chozos N, and Nobles P, "Infrastructure interdependency analysis: Requirements, capabilities and strategy". Adelard document reference: d418/12101/3, issue 1, 2009, available for download at http://www.csr.city.ac.uk/projects/cetifs.html
2. Bloomfield R, Salako K, Wright D, Chozos N, Nobles P, "Infrastructure interdependency analysis: an introductory research review", Adelard document reference D/422/12101/4 issue 1, 2009, available for download at http://www.csr.city.ac.uk/projects/cetifs.html
3. Bloomfield R and Gashi I, Evaluating the resilience and security of boundaryless, evolving socio-technical Systems of Systems, research report fro DSTL, Centre for Software Reliability 2008, available for download at http://www.csr.city.ac.uk/people/ilir.gashi/Papers/2008/DSTL/
4. Buncefield explosion official investigation website, http://www.buncefieldinvestigation.gov.uk/index.htm
5. "The Pitt Review: lessons learned from the 2007 floods", official website http://www.cabinetoffice.gov.uk/thepittreview.aspx
6. Hollnagel, E, Woods D, and Leveson N, eds, "Resilience engineering: concepts and precepts". Ashgate Publishing Company, 2006.
7. Toegepast Natuurwetenschappelijk Onderzoek (TNO), see http://www.tno.nl
8. UK Cabinet Office, Cm 6683, Transformational Government, Enabled by Technology, November 2005
9. Gosh A and Del Rosso M, "The role of private industry and government in critical infrastructure protection, 1999. see http://gost.isi.edu/cctws/delroso-ghosh.PDF
10. International Telecommunication Union, "Creating Trust in Critical Infrastructures workshop", 2002, see http://www.itu.int/osg/spu/ni/security/