On the Safety Implications of e-Governance: Assessing the Hazards of Enterprise Information Architectures in Safety-Critical Applications

C.W. Johnson and S. Raue,

Department of Computing Science, University of Glasgow, Scotland.
{johnson, raues}@dcs.gla.ac.uk

Abstract. Governments across Europe and North America have recently reviewed the ways in which they provide both the public and their own departments with access to electronic data. Information service architectures have been proposed as one important component of the new e-Governance visions. These web-based technologies offer huge benefits by defining common interfaces between different information systems, enabling government services to share information with the members of the public and among each other. However, the introduction of e-Governance architectures also creates a number of concerns. Inaccuracies or errors can be propagated well beyond the organizations that are responsible for maintaining the resource. There is also a concern that data, which was originally gathered for general applications, will be integrated into safety-critical systems without the corresponding levels of assurance or data integrity. This paper advocates the creation of a code of practice for the digital dissemination of safety-related information across government departments.

Keywords: e-Governance, Data Integrity, Safety Information, Emergency Planning

1 Introduction

Relatively little attention has been paid to the safety-related hazards that arise from the integration of government information sources. This is a significant omission given that demographic data and infrastructure information inform the deployment of emergency services as well as the allocation of healthcare resources. Rather than focusing on the safety-related concerns of e-Governance, attention has focused on reducing costs and increasing social inclusion through the provision of networked information services.

1.1 E-Governance and the Focus on Cost Reduction

UNESCO defines e-Governance to be the ‘use of ICT by different actors of the society with the aim to improve their access to information and to build their

capacities'[1]. The UK government began the sustained development of resources in this area during the mid 1990s. These initiatives were mainly focused on data provision to the public. However, they suffered from a lack of coordination. In consequence, there was a proliferation of web domains that were "disconnected and relatively hard to navigate" [1]. These problems were compounded by political pressure to move more information on-line. In 1997, Prime Minister Tony Blair promised that 25% of government business would be handled electronically by 2002. A key motivation in the program was the perceived need to reduce the costs of central government [2]. It was argued that each year, the Department of Social Security could save £7.7m by moving 2% of its 160 million phone calls to its website. However, this initiative was again marred by a lack of joined-up thinking. For example, some departments included telephone call centers within their interpretation of Blair's "electronic" services. There was little integration between the information provided using conventional sources and the emerging web-based systems. Call centre operators lacked training in the government computer-based applications. Only a dozen of the UK Benefit Agency's 75,000 staff could access their own web site from the computers on their desks. A lack of standardized information exchange technologies as well as missing development standards across government departments led to huge variations in the implementation of these systems [3]. The focus was on reducing costs rather than on accuracy, security or reliability of the proposed government information systems.

1.2 E-Governance and the Focus on Coordination of Local Services

National governments have been keen to ensure that local authorities adopt the use of networked information systems. However, the lack of consistency already seen between the departments of central government is often worse between local government agencies [4]. For example, Swedish information infrastructures were characterized by a diversity that stemmed from the decentralized 'commune experiments' of the 1980s. During the budgetary crises of the 1990s, more and more administrative functions were transferred from state level to the regional administrations. A host of web based services were developed to help members of the public access information about these decentralized services. The sites were developed both by local government and also by local citizens groups. Again, however, the diversity of local needs and local provision created inconsistencies that acted as barriers for the future exchange of information between local government and central agencies [5]. Similar patterns can be seen across Germany. Under the Constitution of 1949, the Federal Government was not allowed to establish regional or local field offices to carry out national policies or legislation. In consequence around 6% of public sector workers were employed at the federal level, 50% were employed by the Länder and 40% by local government. As in Sweden, this created a legacy of sub-regional information services that hinders integration. The examples of Sweden and Germany show how European states have focused on the need to improve the integration of national and regional government information infrastructures rather than considering potential safety implications.

[1] See http://portal.unesco.org/, Last accessed June 2010.

1.3 E-Governance and the Focus on Individual Information Portals

The early proponents of electronic government argued that this technology would revolutionize public access to administrative and financial information [1]. No longer would citizens have to go to government departments during office hours and wait for hours to find that the forms were held in another office. In the future, it would be possible to directly access the required information in a matter of seconds through individual information portals. In contrast, many European states suffered from a proliferation of local and central government web sites. Individuals had to spend increasing amounts of time navigating between web sites for Parents Online; Supporting People Strategies Toolkit; Floor Targets Interactive; Interactive Whiteboards Catalogue; UK Man and Biosphere; Government Decontamination Service; Home Information Pack; Drinking Water Inspectorate; Civil Service Statistics. In the UK this led to a cull of domain names. Fewer than 30 sites were retained from a total of more than 900. The public were redirected though a Directgov portal for most individual information requirements and a business link portal for commercial needs. In France, the mon.service-public.fr domain extended the existing Minitel infrastructure. The intention was to provide every citizen with a personal internet portal through which they could pay taxes, register a child for a state school, check the status of car registrations etc. The emphasis on consistency and centralization in other European states can be contrasted with moves towards e-Governance in France. In particular, there was a perceived need to "move away from a traditional mindset of dependency on the central ministries towards one where the field services could exercise greater autonomy in their operational management and be held more accountable for their own actions" [6]. However, as in Sweden, Germany and the UK, the emphasis was on reducing costs and enabling public access. This obscured concerns that the integration of government data services might have implications for public safety.

1.4 E-Governance and the Focus on Social Inclusion

Safety concerns have, however, been raised as part of wider arguments about social inclusion. Individuals may be placed at increased risk if they cannot access electronic information about healthcare services, faulty products, etc. [2]. For example, many government sites still cannot be accessed by those with a visual impairment because they cannot be translated using screen reading software. Other government sites cannot be accessed by linguistic minorities because they are only published in the language of the majority population. The problems of social inclusion also extend to low income groups who often lack the equipment and domestic stability necessary to access on-line information systems. These sections of society often have the greatest need for government information services. The concerns extend well beyond European member states. According to the latest figures published in the Global Information Technology Report 2009-2010 only 4.4% of the Indian population has access to the internet. At the same time, the southern Indian state of Andhra Pradesh has invested some $5.5m in their SmartGOV initiative. This is intended to put all local government services online. The two main objectives are again to cut 'red tape' and reduce costs for the taxpayers.

1.5 E-Governance and the Focus on Security

E-Governance initiatives have been supported by legal innovations, such as the recognition of digital signatures in French law during March 2001. These provisions support the transfer of many financial and administrative services to emerging web-based infrastructures. However, legal changes also reinforce concerns over the security of network transactions. Early denial of service attacks prompted President Clinton to establish a series of public-private partnerships that were designed to prevent an 'electronic Pearl Harbor'. In 2000, the US Government invested some $1.75 billion to safeguard the .gov infrastructure. President Obama has continued to increase expenditure in this area through the development of a renewed cyber-security program in 2009 [7]. The focus on cost savings, on regional information dissemination, on social inclusion and on security are instructive because they have arguably obscured the safety threats posed by future plans for the integration of government information services.

2 E-Governance and Concerns over Public Safety

One means of assessing the utility and usability of government information services is to consider the support that they provide for citizens during an emergency. For example, the need to improve government information services for safety critical applications can be illustrated by problems that faced the public and emergency personnel during the UK floods in 2007. Subsequent sections identify potential solutions to these problems through the use of distributed information management between government departments. This is illustrated by a case study in resource allocation for Fire and Rescue Services.

2.1 Problems of Distributed Information Management: UK Floods (2007)

The UK floods of 2007 provide an appropriate case study in the safety concerns associated with e-Governance because many different local and national agencies struggled to provide first responders, planners and individual citizens with information to combat a series of extreme events. The floods were triggered by heavy rainfall that exacerbated high levels of ground water. This combination overwhelmed drains and other forms of flood defense. The UK Meteorological Office recorded 414.1mm of rain across England and Wales; this was more than double the mean expected level of rainfall. The independent report into the subsequent floods, chaired by Sir Michael Pitt [8], argued that these events created "a new level of challenge" for emergency personnel; triggering "a series of emergencies which stretched local resources to the limit" and provided UK civil contingency planners with a "wake-up call". The floods caused 13 deaths as well as damage to over 40,000 homes and 10,000 businesses. Areas of the UK national rail network were disabled. At the same time, approximately 10,000 motorists were stranded by the closure of part of the M5 motorway.

Confusion, contradiction and inconsistency characterized many aspects of the information interchange that took place between local and national agencies during

the floods. The UK Cabinet Office had an almost continual need for information from local agencies to help form the 'big picture' during these floods. The Cabinet Office is a department of the Government of the United Kingdom responsible for supporting the Prime Minister and Cabinet. It has a coordinating role across different branches of government, in particular via the Cabinet Office Briefing Room (COBR) crisis response committee. This committee guides the government's response to major contingencies. However, their information requests were not always synchronized by regional government so that some key individuals became swamped by requests for information [9]. At the same time, local agencies often did not prioritize these requests from national agencies if they were not perceived to help the people caught up in local flooding. Central government, therefore, found it hard to estimate how many people had been affected by the floods. Initial reports from the Environment Agency suggested that between 3,000 and 4,000 properties were affected. Several days later, Government Offices and local authorities reported that 30,000 houses were flooded. The discrepancy arose because the Environment Agency only counted properties affected by river flooding. It excluded surface water flooding of urban properties even though this was the most significant source of damage.

One reason for the devolution of e-Governance responsibilities during the 1990s from national to local agencies was that they were best equipped to meet the information requirements of the local population. However, local agencies had a 'poor understanding of the location of critical sites; the mapping of their vulnerability to flooding; the consequences of their loss; and dependencies on other critical infrastructure' [8]. There was a need for first responders to have up-to-date flood risk information to coordinate their efforts in helping the public. This data was also important to ensure that emergency personnel did not expose themselves or their vehicles to additional hazards. Local risk assessments created a requirement to integrate national meteorological forecasting, with environmental and urban models that considered critical infrastructures. Responders had to access warnings issued by many other agencies, for example to ensure that they were aware of changes in the level of a water course, or to determine whether or not a power cable was live, or to determine the degree of risk posed by structural damage to a dam. These problems stem from the institutional and organizational barriers to information interchange that are a legacy of the piecemeal manner in which most European and North American governments created their information infrastructures. For example, different UK government agencies use different mapping tools and file formats during the development of Geographical Information Systems. This makes it difficult to share data – for instance about flood levels and the location of 'at risk' members of the public or the location of Fire and Rescue Personnel and the state of local critical infrastructures.

These same problems of information exchange not only affected government agencies, they also had a direct impact on the safety of the general public. During the UK floods, one family saw water pour through the door of their home. They asked the local government agency or council for sandbags, which arrived one week later. This was after their property had sustained significant water damage. When the father called the local Fire and Rescue Service, he was put through to a different county. They were unable to provide any help as he tried to evacuate his family from the rising flood waters. He, therefore, again telephoned the local council and was told to

go to a nearby leisure centre. He drove his family at some risk through the flood waters only to find that had been given the wrong information. The leisure centre was not being used as an evacuation point. One businessman noted that "The websites don't actually say [this] car park is going to flood – it's this tributary and that confluence – for people who don't have a geographical knowledge of rivers, it's almost impossible to weigh what's at threat and what's not" [9]. Individuals were forced to search through dozens of web sites to find information about insurance claims, about whether or not they could drink the water in their mains supply, about the disconnection or restoration of electricity; about the risk of further flooding. These sites were usually overloaded with enquiries and response times were very poor.

Natural disasters such as the 2007 floods provide important insights into the information needs of government agencies and of the general public. They also illustrate the difficulty of identifying whether data is 'safety-critical' or not. Information about the capacity and location of supermarket car parks gain importance when it is used to coordinate evacuation activities. Conversely, it becomes very difficult for information providers to identify those members of the public with the greatest needs, as they seek to protect their families, from those individuals who have more mundane requests. A range of government initiatives offer the potential to address these concerns – for instance through the extension of common information architectures.

2.2 Opportunities for Distributed Information Management: Integrated Risk Management Planning

The floods of 2007 illustrate problems in the dissemination of safety-related information between Government Departments. In contrast, the potential benefits of e-Governance can be illustrated by recent attempts to integrate diverse data sources to support the allocation of emergency services. In the UK, much of this work has been driven by a policy decision to use risk assessment to inform strategic planning by the Fire and Rescue Services (FRS). This approach is embedded within the Integrated Risk Management Plans (IRMPs) that document the deployment of FRS resources to fight and prevent fires but also to support the public during natural disasters, including floods, and terrorist attacks. The aim of IRMPs is to improve community safety and make a more effective use of FRS resources by: "reducing the incidence of fires; reducing loss of life in fires and accidents; reducing the number and severity of injuries; safeguarding the environment and protecting the national heritage; and providing communities with value for money". The development of an IRMP requires data from a range of different government agencies including but not limited to the Department of Communities and Local Government (CLG), the Home Office, and the Office of the Deputy Prime Minister [10, 11 and 12]. For instance, information is required about the population at risk – this implies demographic data from census statistics together with, for instance, information about the occupancy and use of business premises. It is also important to consider whether there are any special hazards within a particular location, including petrochemical storage facilities or manufacturing plants. The allocation of FRS resources must also consider vulnerable locations including hospitals or care homes. These approaches also require information about the likelihood and consequences of future fires, informed

by data about previous losses. In addition, risk based planning must draw on government information about the effectiveness of prevention and protection measures including structural fire resistance, means of escape, sprinkler systems, automatic detectors and alarms, fire doors, ventilation systems etc. Decisions about the deployment of fire resources, vehicles and people, also need to be informed by data on road traffic congestion in order to predict response times.

The complexity of gathering all of this information from various government departments has resulted in the development of software tools to support the Fire and Rescue Services. For example, the Fire Service Emergency Cover (FSEC) tool helps to assess risk, plan response, and model the consequences of different resource allocations for emergency events. Similarly, Figure 1 illustrates a tool to help analyze the risks created by false alarms. This integrates information about previous fires, about the probability of false alarms in a particular region together with the costs of deployment for fire-fighting appliances. The intention is to help FRS planners identify optimum tactics in response to future alarms. Such tools can be used to assess whether or not to send a large number of fire appliances to a location with a known history of previous false alarms. The risk-based approach to planning is important because the answer to such a question depends, in part, upon the people and property that would be threatened by a potential fire.

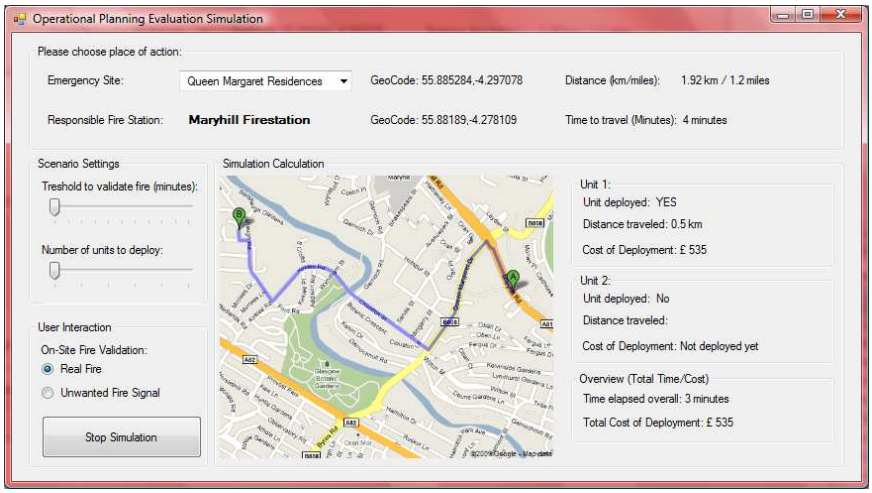

Fig. 1. Possible User-Interface for conducting Operational Planning Evaluations (Raue and Johnson, [11])

These initial steps towards information integration have introduced further research challenges. How can we assess whether the deployment of additional staff and equipment has helped to reduce the number of fatalities/building loss that might otherwise occur? How can we validate the information used to inform our predictions when much of the underlying Government data was never intended to be used in safety-related systems? It is difficult to gather the data required by this new generation of safety-related tools for e-Governance. Each FRS in England collects data in different formats to support their existing systems and processes. This makes it

difficult to update the data that is exploited in tools such as that illustrated in Figure 1. The data from each area must first be converted into common formats before the information is introduced into a periodic update. New copies of the FSEC application are distributed to end users in timescales that are measured in years and not months. In most situations this is not significant; however, it can create problems for instance when industrial units change their operations, when buildings change their occupancy levels or when new housing developments create entirely new demands on the FRS.

3 The Safety of Future Government Information Architectures

Both the U.K. [13] and U.S. governments [14] have recently reviewed their provision of electronic information. Web service architectures have been proposed as an important component within new visions for e-Governance. The W3C define a web service to be a software system that supports 'interoperable machine-to-machine interaction over a network'. Other systems interact with the web service using a prescribed interface over Simple Object Access Protocol (SOAP) messages based on HTTP with XML serialization. These technologies offer considerable benefits including mechanisms for the integration of government information services. This, in turn, has important implications for safety-related applications, such as those introduced in the previous section.

3.1 The UK Government's Enterprise Information Architecture (xGEA)

Recent e-Governance initiatives can be illustrated by proposals for the UK Government's Enterprise Information Architecture (xGEA) [15]. This is intended to provide a reference model that can help to 'align existing and emerging technical architectures across government'. It was also intended to broaden and deepen the government's 'professionalism' in the provision of information services. The use of this term is significant given the limitations identified with previous public IT procurements [1, 2 and 7]. The xGEA ~~architecture~~ is intended to support three primary objectives:

- 'To reuse solutions developed for specific issues but which potentially could have a wider value' [15]. This has clear implications for the manner in which tools such as FSEC have re-used demographic and road traffic data to support safety related decision making in the Fire and Rescue Services.
- 'To share across public sector organization boundaries to work more efficiently and save resources' [15]. This again is important given that barriers exist not simply in terms of the hardware and software used across different Government departments but also in terms of the different data formats used, for example by different English FRS. Previous sections have also described similar barriers in many other EU member states hence we would argue that this is a generic aim to be shared across many different countries.
- 'To be informed of the wider context (other public sector bodies, business and the citizen) in which IT enabled business change is taking place' [15]. This is

a significant aim behind the xGEA initiative because public information systems have tended to lag behind private sector innovations.

These themes of sharing and re-use are critical because they create the opportunities for safety-related decisions to be better informed by the integration of data from across government departments. At the same time, these innovations renew concerns about the integrity and application of this information, when it may not originally have been intended for such uses. An xGEA Reference Model (xGEARM) has been developed in order to support the reuse and integration of information across government, through an agreed set of terms and definitions. The key components of this model are illustrated in Figure 2 [15]. At the time of writing, work is continuing to develop the technical and architectural details of each of the domains mentioned in this diagram. As can be seen, the issues of information assurance and integrity are not explicitly represented at this top level.

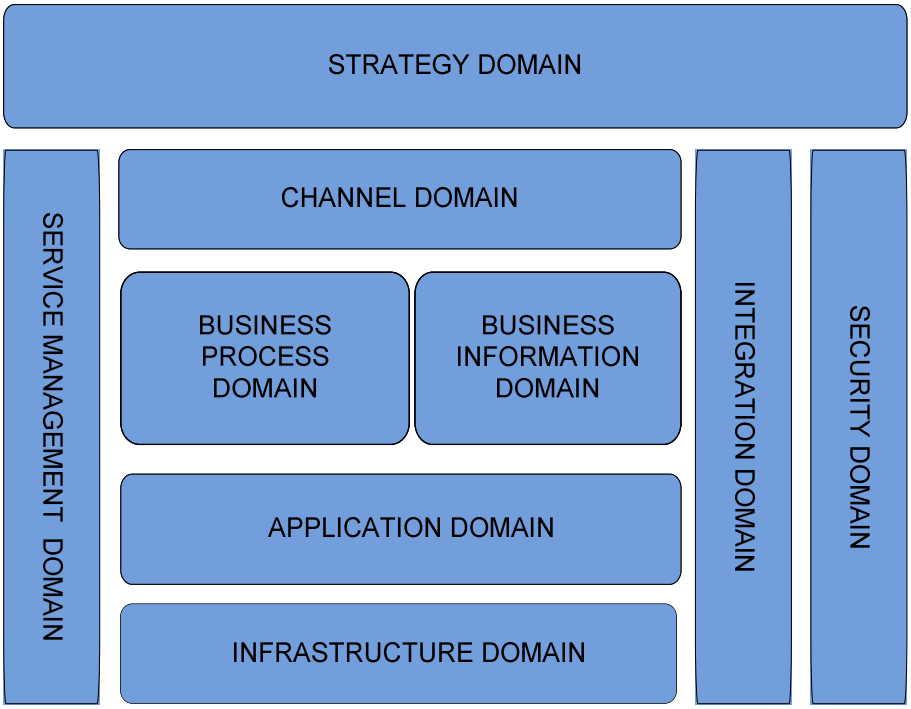

Fig. 2. The UK Government's Enterprise Information Architecture Reference Model (xGEARM)

One of the key concepts in xGEA is a repository that will collect case studies of the ways in which departments can exchange data. More generally, these case studies can also provide examples of the exchange of 'leading practices' or business processes. UK Cabinet Office documentation identifies four initial types of exemplar. These include a Managed Service built using existing staff and technical resources. They also include Solution exemplars. These require additional investments but are based on proven techniques. A third form of 'exemplar' provides patterns that can be

followed again. Finally, Lesson Learned provide ‘a set of recommendations around a specific area’. The initial exemplars to be held within the xGEA were selected in terms of their value to government defined in terms of:

- “Cost saving – e.g. investment has already been made and can be reused with little further expense;
- Cost avoidance – e.g. in a future planned program driving down its costs;
- Increase quality – reuse an existing solution/service that has already been tested;
- Time to market – reuse an existing solution/service that has been built
- Increased function to citizen – additional functionality not previously envisaged may be available
- Increase citizen access to government – access to more citizens than first envisaged may be possible” [15]

Safety concerns over data integrity and accuracy are covered within data quality. However, the observation that this will ‘reuse an existing solution/service that has already been built’ would seem to focus again on the issues of cost that are already listed as the first item in this enumeration of value within the enterprise architecture.

The UK government have also identified a process by which xGEA supports the exchange of information across government. The identification of business needs leads to a sustained search across the repository of previous exemplars to provide a template for exchange. This is then placed within the broader context of the xGEA, for instance by mapping elements of the case study to components of xGEARM in Figure 2. This is important because the exchange of information and processes must, in turn, support further sharing with other departments who might themselves, in turn, benefit from any new application. The final stage is to deliver the service provision within the end user organization. It is, therefore, critical that anyone re-using an exemplar for a safety-related application conduct a formal risk assessment to consider the potential hazards from re-use. These include an over-reliance on data that has not been adequately validated or independently verified. They also include the problems of re-using obsolete information. There are further concerns about whether subsequent users of government information understand the semantics of the data items that are being re-used to inform life critical decisions.

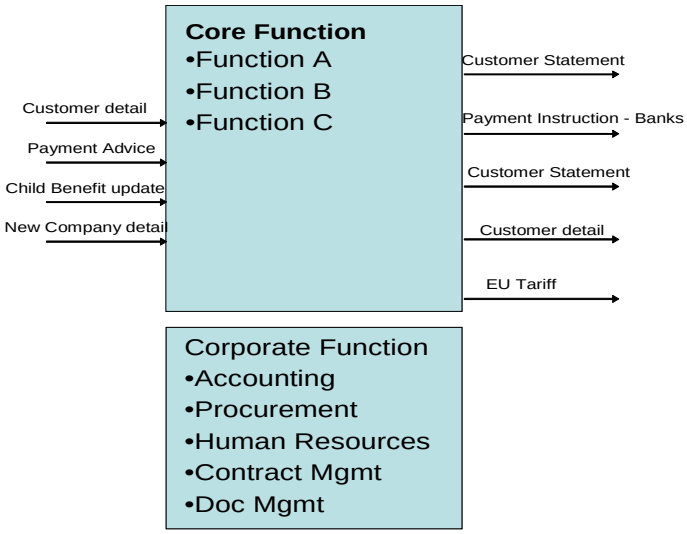

Fig. 3. An Example of a Top-Level Business Process View of Core Functions within xGEA

Figure 3 illustrates the top-down functional modeling that has been proposed to identify areas for information sharing across government. The lower box illustrates the corporate functions that support the transformations illustrated by the upper box. Functions A, B and C depend on underlying accounting, procurement, human resource, contract and document management infrastructures. The UK Government's Chief Information Officer argues that "In describing the Business Function model and then comparing it with that from another organization, a number of organizations can be seen to perform a similar function or similar information flow, such as 'Payment Instruction'. This could highlight a potential exemplar that could be used across organizations, which perform similar functions" [13]. However, such an approach requires considerable additional work in order to identify the key constraints that hold over those information flows. In the context of this paper, we might need to ensure that safety-related data was timely, reliable, accurate etc. in addition to the requirement to maintain these functional relationships. It is important not to view the previous paragraphs as direct criticisms of the xGEA. The intention is to identify generic lessons as many different States extend the integration of electronic data to plan their provision of safety-related services. As we have seen, concerns over data integrity and accuracy are not isolated within the United Kingdom.

3.2 A Proposal for Government Enterprise Integrity Requirements

Many government agencies already operate information assurance guidelines that might inform these proposed architectures for data integration. For example, the UK Statistics Authority, Code of Practice for Official Statistics [16] provides eight principles:

- **Principle 1: Meeting user needs.** The production, management and dissemination of official statistics should meet the requirements of informed decision-making by government, public services, business, researchers and the public.

- **Principle 2: Impartiality and objectivity.** Official statistics, and information about statistical processes, should be managed impartially and objectively.

- **Principle 3: Integrity.** At all stages in the production, management and dissemination of official statistics, the public interest should prevail over organizational, political or personal interests.

- **Principle 4: Sound methods and assured quality.** Statistical methods should be consistent with scientific principles and internationally recognized best practices, and be fully documented. Quality should be monitored and assured taking account of internationally agreed practices.

- **Principle 5: Confidentiality.** Private information about individual persons (including bodies corporate) compiled in the production of official statistics is confidential, and should be used for statistical purposes only.

- **Principle 6: Proportionate burden.** The cost burden on data suppliers should not be excessive and should be assessed relative to the benefits arising from the use of the statistics.

- **Principle 7: Resources**. The resources made available for statistical activities should be sufficient to meet the requirements of this Code and should be used efficiently and effectively.

- **Principle 8: Frankness and accessibility.** Official statistics, accompanied by full and frank commentary, should be readily accessible to all users.

These principles provide a template for the development of a more general set of requirements that might be imposed across the data that is to be provided using government information architectures such as those described in the previous section. In particular, we could build upon principle 4 to identify a number of more detailed requirements for information assurance in areas where data might be used in the aftermath of adverse events, including those identified by the Pitt review of the 2007 floods. Similarly, principle 8 might be developed to enable users to benefit from the 'self descriptive' elements of more recent information architectures. Subsequent users of any information should be warned about the potential risks or limitations of applying that data to inform safety-related decisions [17]. For instance, the following principles might be adopted by many different States as they seek to integrate their e-Governance infrastructures:

- **Safety Information Service Principle 1: Transparency.** It should be possible to identify the original source of data that is derived from other government or external agencies. This is especially important when information may be derived from an information service provided by another

department, which in turn is derived from yet another information service. This is a non-trivial issue. For example, information from the Environment Agency about the number of premises affected by a flood may be integrated into FRS planning tools, similar to those described in previous sections. However, the flood data may itself depend upon mapping information and building occupancy data provided by other branches of government. It is difficult, if not impossible, for end users to assess the integrity of this information if they cannot trace these interdependencies.

- **Safety Information Service Principle 2: Applicability.** Ideally, any information provided by a government department should come with the level of assurance that would enable its application to safety-related decisions. However, lack of funding or access constraints can limit the applicability of information services. It may not be possible to conduct detailed site surveys to assess the level of flood protection provided for every water course in the country. Similarly, it may not be possible to accurately measure the traffic delays for every section of road over different times of day. In consequence, the development of national information services often requires the use of extrapolation based on limited sampling techniques. For the end users of this information, it is critical that they can judge the level of confidence that is associated with the use of these sampling and extrapolation techniques when lives may depend upon a data service.

- **Safety Information Service Principle 3: Recency.** The advent of integrated information services creates complex data dependencies. One of the benefits of this approach is that any updates to information services can be automatically propagated to the different departments who are end users of that service. However, this creates a host of further problems. For instance, the same information request can yield radically different results depending on whether the system was using third-party data provided before or after an update. In many instances, the impact of this update may not be visible to the user unless they understand the many complex ways in which information services interact to support decision making tools. For example, updating demographic information will affect fire risk assessments even though no strategic or operational changes have been made. Additional problems can arise if a third party service changes the format or semantics of data etc.

- **Safety Information Service Principle 4: Triangulation.** Safety-related information should be confirmed by reference to more than one data source. This goes beyond data redundancy because triangulation suggests a complementary data source that is independent of a primary information channel. This increases resilience against the problems of sampling bias. It also provides additional warnings should changes be made in the methodologies used to derive data from any individual source, for instance by comparison of the data derived from two independent sources. The implementation of this principle implies additional costs in cross-checking data sources. However, we would argue that for many safety-related

decisions it is worth meeting the additional overheads implied by data triangulation.

It is important to stress that this is a partial list. Additional assurance requirements will be needed as we develop more complex information architectures for the reuse of data between different government departments. For example, the UNOOSA and EGNOS projects are delivering a host of location sensitive information services for emergency response that are beyond the scope of this paper [18]. In the meantime, it is critical to enhance the high-level architectures for government information exchange, such as those illustrated in Figures 2 and 3, if they are to support safety-related services.

4 Conclusion and Further Work

Both the U.K. and U.S. governments have recently reviewed the ways in which they provide access to electronic sources of information. Web service architectures have been proposed as an important component within these new visions for e-Governance. This technology offers huge benefits. In particular, it encourages the provision of joined-up information services that have important implications for a range of safety-related applications. The recent Pitt review into the UK floods of 2007, described how additional risks were created for the public because government agencies did not use compatible Geographical Information Systems. In contrast, web service architectures help to define standardized interfaces between different government information systems. This provides renewed hope of being able to integrate the various resources held by the Meteorological Office, the Environment Agency, the Fire and Rescue Services etc.

The development of novel architectures for e-Governance also creates a number of concerns. It is important to ensure the integrity of data that is shared between many different agencies. Inaccuracies or errors can be propagated well beyond the organizations that are responsible for maintaining the resource. Data, which was originally gathered for general applications, can be integrated into safety-critical applications without the corresponding levels of assurance or data integrity. This paper has described how these issues have arisen during the development of a web service architecture for emergency planning by Fire and Rescue Services. A range of innovative software helps planners to integrate information about demographics, about transportation infrastructures and about fire risks. These tools help to identify the costs and benefits of moving emergency resources, or of allocating greater attention to fire prevention measures.

The concerns identified in our case studies are increasingly important as governments develop service oriented architectures that resolve many of the technical barriers to data integration. We have, therefore, advocated a code of practice for the exchange of government information in safety-related applications. In particular, we introduce the principles of transparency, applicability, recency and triangulation as means of providing the necessary level of information assurance for critical decision making. Transparency deals with the need to identify the source of third party information. Applicability deals with the need to identify caveats and constraints on

the use of information services for applications that are very different from those for which they were originally developed. Recency deals with a host of update problems that can arise, for instance, when safety-critical information is subject to radical changes before and after updates on underlying third party data. Triangulation refers to the need to increase confidence in information sources, ideally by cross-referring data from more than one data sources.

The intention here is not to provide an exhaustive list of data assurance principles but to start a dialogue. Further work is also required to determine whether 'data fusion' and information integration will support safety-critical decision making by European governments. There is a danger that end users will be overwhelmed by a mass of additional information that serves more to confuse than to enlighten. Unless we begin to address the assurance of Government information architectures then there is a danger that many critical decisions will be based on partial or biased information that was never intended for use within safety-related applications.

Acknowledgement

The work described in the paper has been supported by the UK Engineering and Physical Sciences Research Council grant G026076/1; Evaluation of Prevention and Protection Activities On Commercial, Public and Heritage Buildings.

References

1. UK National Audit Office, Government on the Web, London, UK, December 1999. Available on: http://www.nao.org.uk/publications/9900/government_on_the_web.aspx, Last accessed March 2010.
2. UK National Audit Office, Government on the Internet: Progress in Delivering Information and Services Online, London, UK, July 2007. Available on: http://www.nao.org.uk/publications/0607/government_on_the_internet.aspx, Last accessed June 2010.
3. BBC, Government to Close 551 Websites, Thursday, 11 January 2007. Available on http://news.bbc.co.uk/1/hi/uk_politics/6247703.stm, last accessed March 2010.
4. M. Lind, Olov Östberg and P. Johannisson, Acting Out The Swedish E-Government Action Plan - Mind And Mend The Gaps, International Journal of Public Information Systems, vol 2009:2, pp. 37-60.
5. K. Löfgren, The Governance of E-government. A Governance Perspective on the Swedish E-government Strategy. Public Policy and Administration, 22(3), pp. 335-352. 2008.
6. A. Cole and G. Jones, Reshaping the State: Administrative Reform and New Public Management in France. Governance, 18**,** 567-588. 2005.
7. United States Government Accountability Office, Information Security: Concerted Response Needed to Resolve Persistent Weaknesses, Testimony Before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, U.S. House of Representatives, GAO-10-536T March 2010.
8. Pitt Review learning Lessons from the 2007 Floods (Interim report), Cabinet Office, London, UK, December 2007.

9. C.W. Johnson, Complexity, Structured Chaos and the Importance of Information Management for Mobile Computing in the UK Floods of 2007. In M. Klann (ed.), Mobile Response 2008, Bonn, Germany May 2007, Springer Verlag, Lecture Notes in Computing Science, 5424, 1-11, Berlin, Germany, 2009.
10. Our Fire and Rescue Service, White Paper, Office of the Deputy Prime Minister, 2003.
11. S. Raue and C.W. Johnson, Using Web Service Architectures and Advanced Simulation Tools to Ensure that Cuts in Strategic Funding for Emergency Services Do Not Jeopardize the Safety of Local Communities. Submitted to the Proceedings of the International Systems Safety Society, Minneapolis, USA, in press.
12. Y. He and S. Grubits, A Risk-based Equivalence Approach to Fire Resistance Design for Buildings, Journal of Fire Protection Engineering, 2010 20: 5-26.
13. UK CIO, Enterprise Architecture for UK Government: An overview of the process and deliverables for Release 1, http://www.cabinetoffice.gov.uk/cio/chief_technology_officer.aspx, 2010.
14. US CIO, Enterprise Architecture Assessment Framework v3.0: Improving Agency Performance Using Information and Information Technology, Office of Management and Budget, Washington DC, Available on: http://www.cio.gov/Documents/OMB_EA_Assessment_Framework_v3-0_Dec_2008.pdf, 2008.
15. UK Cabinet Office, Enterprise Architecture for UK Government: An overview of the process and deliverables for Release 1, London, UK, October 2009. Available on: http://www.cabinetoffice.gov.uk/media/153627/enterprise_architecture_uk.doc. Last accessed March 2010.
16. UK Statistics Authority, Code of Practice for Official Statistics, January 2009. Available on http://www.statisticsauthority.gov.uk/assessment/code-of-practice/index.html, last accessed March 2010.
17. R McClatchey, Z Kovacs, F Estrella, J-M Le Goff, L Varga, M Zsenei, The Role of Meta-Objects and Self-Description in an Engineering Data Warehouse, ideas, pp.342, 1999 International Database Engineering and Applications Symposium, 1999.
18. C.W. Johnson and A. Atencia Yepez, Safety Cases for Global Navigation Satellite Systems' Safety of Life (SoL) Applications. Proceedings of the International Association for the Advancement of Space Safety, Huntsville Alabama, NASA/ESA, 2010.