

CONSULTATION ON THE RESILIENCE OF FIRE CONTROLS

Introduction

1. Fire Control Rooms are a key part of the Fire and Rescue Services in Scotland. They are the central command and control facility for handling emergency fire calls and, as such, must be able to operate when faced with both routine and exceptional incidents.
2. In addition to handling calls and directing resources to incidents, staff also have the task of ensuring that cover is maintained across the service area. This can involve directing standby moves whereby resources not involved in an incident can be mobilised to fill the gap created by those that are. This helps to ensure that new incidents can be handled promptly.

Background

3. Each of Scotland's 8 Fire and Rescue Services is served by one main (primary) and one standby (secondary) control room. The table below shows how incidents are distributed between the 8, ranging from D&G handling 1.5% of the total to Strathclyde handling 49.8%.

2006/07	Total no of incidents occurring	Average no of incidents per day	No of staff
Central	5300	15	17
D&G	1742	5	17
Fife	6976	19	21
Grampian	8161	22	31
H&I	5148	14	16
L&B	22098	61	34
Strathclyde	57393	157	68
Tayside	8427	23	21
Total	115245	316	225

Table 1 : Source HM Chief Inspector of Fire Services Annual Report, 2006/07.

4. In 2004, the then Scottish Executive published a report prepared by Mott MacDonald which followed a review of the Fire Control Rooms in Scotland. The review recommended that the number should be reduced from eight to one, two or three on the grounds that larger regional controls would be more resilient in terms of three key requirements, these being service delivery, organisational development and efficiency.
5. In June 2006, the previous administration launched a wide-ranging review of Scotland's emergency preparedness, in particular our preparedness for dealing with simultaneous terrorist attacks in light of lessons learned from the London bombings in 2005. The review was led by the then Chief Inspector of Fire Services, Jeff Ord. The review looked again at all the arguments for and against reducing the number of fire control rooms but in a wider civil contingencies context.
6. The current administration considered these reports together towards the end of 2007 and, after taking into account the views expressed by stakeholders, decided not to take any central action to reduce the number of Fire Control Rooms. However, in order to ensure that our Fire Service Controls are capable of responding to the evolving threats, Ministers wanted

to work with Fire and Rescue Authorities and other stakeholders to consider what needed to be done to improve resilience. Accordingly, in announcing the decision, Ministers undertook to consult on the need to improve the standards of resilience in our Fire Controls Rooms, and to then consider with Fire and Rescue Authorities what should be done to meet these requirements.

Structure of the Consultation

7. The consultation is structured as follows:

- Emergency Call Handling
- Physical Resilience
- Technical Resilience
- Operational Resilience
- Critical National Infrastructure and other issues

8. The first part concerns emergency call handling outwith the fire control network, i.e. prior to the point at which a call is transferred to the Fire and Rescue Service (FRS). While outwith the scope of the resilience standards for Fire Controls that we are looking to draw up, it is nonetheless important to consider this aspect of call handling given that the distinction between FRS and telecoms industry call-handling may not be appreciated by the general public who expect a level of service from the point at which a call is placed.

9. Physical resilience relates to the buildings and sites that are used to house the fire controls, while technical resilience covers the technology that is used to deliver the functionality, e.g. the call handling, command & control and mobilising systems. Operational resilience covers the policies and procedures that govern the operation of a Fire Control, including the fall-back arrangements that would apply in the event of control failure. Finally, the consultation asks where fire control sits in terms of the Critical National Infrastructure and how we might reflect CNI principles in any resilience standard.

Section 1 - Emergency Call Handling

10. 999 emergency calls are received by five BT call centres distributed throughout the UK which, between them, handle approximately 28 million calls per annum. Each BT centre can receive calls from anywhere in the UK. In spate conditions when BT cannot receive a reply from an Emergency Authority (Fire, Police Ambulance etc.) within a set period of time the call will be diverted to a nominated “buddy”, which in the case of a fire-related call is normally another FRS or the Police. Where the volume of calls being received by the “buddy” is severe, BT will make arrangements with other service control rooms to seek agreement to pass calls.

11. On receipt of these calls, a fire control operator will ascertain the location and nature of the incident. If the incident is within the local area they will direct resources accordingly, otherwise they will pass details to the appropriate FRS. Fire control operators can also receive calls relating to Automatic Fire Alarms, emergency calls from non-BT phone operators, direct from other emergency services and non-emergency calls.

Question 1: The re-routing of BT calls can have implications for other parts of the UK. How should spate conditions following a major incident in one part of the country be

handled such that the ability of other parts of the country to respond to further incidents is not impeded?

Question 2: Apart from 999 calls, what effect do other demands have on resilience and how could these be mitigated?

Section 2 - Physical Resilience

12. Physical resilience is about being able to continue to operate the primary control room at full or reduced capacity in the face of a range of fault or event conditions, and at present, includes maintaining a service after evacuating to a (generally) inferior secondary control. Physical resilience should also be considered in a “whole building” context, and not just the control room environment.

13. All critical equipment should be at least duplicated with at least one component being physically remote from the others in the group, thus ensuring the ability to cope with catastrophic failure while still maintaining a full service.

Question 3: Is the current level of infrastructure duplication enough to ensure sufficient resilience? If not, what more could be done?

14. Many Fire Control Rooms are in need of upgrading with the uncertainty surrounding the Mott McDonald review having been responsible for an investment hiatus in some cases. Older Fire Control Rooms may have been established at a time when the nature of the threat that we faced was far removed from what we face today. The more modern controls all benefit from security entry systems, although most of them are also located less than 200m from a public road. Most seem to be at low risk from flooding but we are not aware of e.g. any control that has strengthened roofs or walls.

15. Some Fire Control Rooms are located on or near flight paths. Public Safety Zones are areas of land at the end of the runways at the busiest airports within which development is restricted in order to control the number of people on the ground at risk of death or injury in the event of an accident on take-off or landing. In Scotland, these are currently found at Aberdeen, Edinburgh, Glasgow, Inverness and Prestwick Airports. The basic policy objective governing the restriction on development near civil airports is that there should be no increase in the number of people living, working or congregating in Public Safety Zones and that, over time, the number should be reduced as circumstances allow.

Question 4: In the context of the threats that we face, what physical security measures are appropriate for a Fire Control?

Question 5: What needs to be done to improve resilience in the context of non-technical threats, such as flooding, fire or building impact?

Question 6: Are any controls located within Public Safety Zones? What level of risk should be attributed to a control being hit by an aircraft?

Question 7: How susceptible is your Control to unauthorised public access? What level of risk should be attributed to this?

16. It is good practice for Fire Control Rooms to develop and test appropriate contingency plans to address major incidents, including control room failure.

Section 3 – Technical Resilience

17. Physical security will always be a prime consideration, however in terms of ensuring resilience the risk to the physical integrity of a Fire Control Room represented by terrorism or other such catastrophic event is, while real, less than that posed by the risk of technical failure.

18. Each element of the call handling and mobilising infrastructure is duplicated to ensure resilience, including the ability to receive calls from more than one telephone exchange. Other duplicated elements include:

- Power Supply
- Integrated Command and Control System (ICCS)
- Management Information System
- Mobilising System
- Radio System

19. Minimising the risk of technical failure is clearly important and this is often achieved by building in additional capacity through duplication of the elements listed above.

20. The need to ensure that ICT systems are robust and suitably resilient is recognised in the development of global ICT standards for information security management, such as the ISO/IEC 27000¹ series.

Question 8: Does the current standard of equipment design take sufficient account of the operations-critical nature of the ICT systems used by our Fire and Rescue Services?

Question 9: Does the ISO/IEC 27000 series on information security standards (or any other standard) represent a useful basis for supporting ICT resilience in the Scottish Fire and Rescue Services?

21. Firelink will bring investment to the radio communications aspect of the fire control infrastructure and will result in the Airwave system being interfaced to the 8 FRS Integrated Communications Control Systems (ICCS) . This will unlock some functionality by allowing the mobilising systems to use Airwave to communicate with each Fire Station and to every appliance via mobile data terminals. In return, the control rooms will be able to receive status and Automatic Vehicle Location System (AVLS) information (e.g. “en route”, “arrived at scene”) from the vehicles. Other than that, the project will not involve any direct improvements to mobilising systems or the ICCS. It is worth noting that in the short term, variations in project timetabling could introduce an element of uncertainty where resilience planning is concerned.

1

<http://www.berr.gov.uk/sectors/infosec/infosecadvice/legislationpolicystandards/securitystandards/isoiec27002/page33370.html>

22. The 8 Scottish Fire Control Rooms currently use a range of equipment produced by more than one manufacturer e.g. mobilising systems produced by Fortek (6), Remsdaq(1) and Motorola(1) sitting alongside a similar variety of ICCS. Mixed technology can bring resilience benefits in that a design failure in one technical solution will not impact on the others. However, shared technology can also bring benefits in terms of sharing spares and expertise, the latter being particularly useful where there is a need to deploy operators to another control e.g. in the event of control failure.

Question 10: Would resilience be better served if we started working towards a single technical solution or is it necessary to have variety in order to protect against design failure?

Section 4 - Operational Resilience

23. Having covered physical and technical resilience, this section looks at control staff and working practices.

24. Control rooms will generally experience an increase in demand in the late afternoon / early evening with a corresponding dip in the small hours. Flexible working patterns can provide greater resilience when it comes to coping with this. Spate conditions can occur in the immediate aftermath of an incident (e.g. a vehicle burning on the hard shoulder of the motorway) when the increase in the use of mobile phones can mean that literally hundreds of calls are received over a short period of time. Major incidents can involve all of the above, with the added difficulty of moving resources to fill the gaps in cover created by deploying resources to the incident itself.

Question 11: What steps can be taken to safeguard resilience when dealing with demand variations that are within “normal” operating parameters?

Question 12: What steps are taken and can be taken to maintain resilience when dealing with exceptional demand, e.g. related to a major incident (including the loss of a control room)?

25. Response Standards vary across Scotland, in large part based on Integrated Risk Management Plans that have been agreed in the context of local risks. Also certain legal duties and obligations fall upon to the Chief Fire Officer and Fire Boards. It could be argued that these issues represent a barrier to staff assuming responsibility for calls in another Fire Service area.

Question 13: In the context of a controller from one area mobilising resources in another, how big a barrier does different response standards represent? Can more be done to harmonise response standards or do these properly reflect local needs? Are there any other issues which may affect the ability of a controller from one area mobilising resources in another?

Local Knowledge

26. Views vary on the importance of local knowledge to the work of a fire control operator. Most contend that it is essential to understand the quirks and vagaries of the service

area (e.g. there are at least three roads called “Princes Street” in the Lothian & Borders area). That said, controllers themselves recognise the need to guard against making assumptions around what they are being told and firefighters on the ground working out of local stations have much to bring to the table. Technology continues to develop to help bring safeguards to fire control work (e.g. Gazeteers linked to Calling Line Identity systems). There is also a view that the key aspect of “local knowledge” is in fact good teamwork between the controller and the crews built on a working relationship which is based on mutual respect which can take time to establish.

Question 14: What do you understand by “local knowledge”, where does it primarily reside, and how important do you think it is to underpinning resilience?

Secondary Control Rooms

27. In the event of maintenance work, catastrophic technical failure or if premises have in any other way been compromised, it may be necessary to abandon (wholly or partly) a primary control.

28. Each FRS in Scotland currently operates a primary and secondary control, with the latter being on standby in the event of the former failing. The ability to use another primary control as the fallback option has been limited in the past because of technical compatibility issues. However Firelink and other investment will bring improvements to this area. It is clear that the functionality in secondary controls is generally poorer (utilising whiteboards rather than real-time wall-screens, old equipment etc.) which militates against a seamless transition.

29. There are some wider issues in relation to back-up controls that go beyond the ability to make a seamless switch. One view is that a secondary control should be geographically remote so that e.g. there is less chance of the physical conditions that compromised the primary having a similar effect on the secondary. Most secondary controls are currently in close proximity to the primary as the (possibly unsafe) working assumption is that the same staff would end up operating both.

30. Enabling the 8 primary controls to be linked together as a single virtual control might help in this respect. Such an approach would allow the residual capability which currently resides in each of the 8 control rooms to be utilised in the event of the loss of any primary control. This approach has the potential to offer a more cost-effective solution to maintaining 8 surplus controls, however it is not without operational and technical challenges. Technical issues aside, one of the key operational issues would be how the virtual control could be configured so as to accommodate the loss of the Strathclyde control room and its significant share of Scotland's call volume

Question 15: Would resilience be helped if the default fallback was to another primary control rather than a standby secondary control? How would this work with respect to the largest primary control?

Question 16: Does Scotland need 8 secondary controls in order to be resilient? How many secondary controls are required and what capacity should they/it have? Where should a / these secondary control(s) be located?

Question 17: Where control failure is concerned, what steps can be taken to help ensure collective resilience?

Section 5 - Critical National Infrastructure (CNI) and other issues

31. CNI refers to the key elements of the national infrastructure which are crucial to the continued delivery of essential services to the UK. Essential services are delivered by the communications, emergency services, energy, finance, food, government, health, transport and water sectors. Without these services, the UK could suffer serious consequences, including severe economic damage, grave social disruption, or even large scale loss of life.

32. The Centre for Protection of National Infrastructure² bases its work around 10 key guidelines:

- assess the risks to your business
- consider security first when planning building works
- establish a security culture in your business
- keep premises clear and tidy
- control access points and use staff and visitor passes
- install physical measures e.g. locks, alarms, CCTV, lighting etc
- establish good mail handling procedures
- recruit carefully, checking identities and following up references
- take proper IT security precautions
- test your business continuity plans regularly

Question 18: How could existing Fire Controls be improved in the context of the 10 CPNI guidelines?

33. Annex A sets out some resilience good practice that applies to all elements of the Critical National Infrastructure.

Question 19: Are these good practice examples relevant to our consideration of fire control resilience in Scotland?

34. The publication of this consultation document represents the first stage in this process is to gather the views on the need to improve the standards of resilience in Scotland's fire control rooms. We welcome comments and input from all parties and look forward to receiving views.

Question 20: Are there any issues that you want to raise covering how physical, technical and operational resilience overlap?

Question 21: Are there any other points that you wish to make in relation to ensuring the resilience of our fire control rooms or about this exercise more generally?

² www.cpn.gov.uk

Question 22: Finally, are there any points that you want to make in terms of how any resilience standard might be implemented?

Conclusion

35. In November 2007 the Scottish Government announced that it would not be taking any central action to reduce the number of control rooms in Scotland. In making that decision, account was taken of the various reviews previously undertaken and the strong local views expressed by stakeholders on the importance of local control rooms. However, it was also recognised that there remains a need to ensure that our control infrastructure is capable of responding the changing threats we now face and whether there is a need to improve our collective resilience. Thus, in taking this decision, Ministers undertook to consult on the need to improve the standards of resilience our controls rooms can provide, and to then consider in partnership with Fire and Rescue Authorities what should be done to meet these requirements.

36. The publication of this consultation paper represents the first stage in that process.

Scottish Resilience

May 2008

Resilience Good Practice for CNI elements

Carry out regular risk assessments to decide on the threats you might be facing and their likelihood. Identify your vulnerabilities and the potential impact of exploitation

When acquiring or extending premises, consider security at the planning stage

Make security awareness part of your organisation's culture and ensure security is represented at a senior level

Ensure good basic housekeeping throughout your premises. Keep public areas tidy and well-lit, remove unnecessary furniture and keep garden areas clear

Keep access points to a minimum and issue staff and visitors with passes. Where possible, do not allow unauthorised vehicles close to your building

Install appropriate physical measures such as locks, alarms, CCTV surveillance, complementary lighting and glazing protection

Keep mail-handling procedures under review

When recruiting staff or hiring contractors, check identities and follow up references

Consider how best to protect your information and take proper IT security precautions.

Examine your methods for disposing of confidential waste

Plan and test your business continuity plans, ensuring that you can continue to function without access to your main premises and IT systems.