Evidence:

Using safety cases in industry and healthcare

A pragmatic review of the use of safety cases in safety-critical industries – lessons and prerequisites for their application in healthcare

December 2012

Identify Innovate Demonstrate Encourage

This research was commissioned and funded by the Health Foundation to help identify where and how improvements in healthcare quality can be made. The views expressed in this report do not necessarily represent the views of the Health Foundation.

This research was managed by:

Jonathan Riddell Bamber, Research and Development Manager
The Health Foundation

jonathan.bamber@health.org.uk
020 7257 8000

Project team

Prof Robin Bloomfield, Centre for Software Reliability, City University, London; Adelard LLP, London

Dr Nick Chozos, Adelard LLP, London

Dr David Embrey, Human Reliability Associates, Wigan

Jamie Henderson, Human Reliability Associates Wigan

Dr Tim Kelly, Department of Computer Science, University of York

Dr Floor Koornneef, Safety Science Group, TU Delft, Netherlands

Alberto Pasquini, Deep Blue Research & Consulting srl, Rome, Italy

Dr Simone Pozzi, Deep Blue Research & Consulting srl, Rome, Italy

Dr Mark-Alexander Sujan, Warwick Medical School, University of Warwick

Contributing authors

Dr George Cleland, Adelard LLP, London

Ibrahim Habli, Department of Computer Science, University of York

Dr John Medhurst, Human Reliability Associates, Wigan

Contact

Dr Mark-Alexander Sujan
Warwick Medical School
University of Warwick
Coventry, CV4 7AL

m-a.sujan@warwick.ac.uk

Evidence: Using safety cases in industry and healthcare is published by the Health Foundation, 90 Long Acre, London WC2E 9RA

ISBN 978-1-906461-43-0

Contents

Health Foundation commentary

The twelve years since the publication of *An Organisation with a Memory*[*] have seen important steps in the development of practices to improve patient safety in the UK. There has been an increased recognition of the responsibility for improving patient safety at every level of the system. Work done across the UK, supported by the Health Foundation and others, has challenged the view that some patient harms are inevitable.

Healthcare is a process, with a number of interrelated interventions leading to a particular outcome. For example, for a patient to receive the correct medication there is a process in which a drug is first prescribed, then dispensed and then administered. In order for safe medication treatment to occur, each of these steps must be completed correctly. However, as shown by the Health Foundation's report, *How safe are clinical systems?*, the reliability of care pathways can vary even within the same organisation, with between 13% and 19% of care processes failing to be completed to the agreed standard every time.[†]

Over one hundred years ago Florence Nightingale collected evidence of mortality during the Crimean war to determine which hospitals were safe. Currently the National Reporting and Learning System (NRLS) provides invaluable information about hazards, risks and actual cases of patient harm across the NHS in England and Wales. Such measures have been used to assess performance against national and local targets by both commissioners and regulators; however, a number of recent high-profile failures within the NHS have demonstrated that measuring compliance with standards is not enough. The publication of the Mid Staffordshire NHS Foundation Trust Public Inquiry, due in 2013, will trigger a discussion about how we can be sure that care is actually safe, rather than waiting for errors to occur.

Having learned from running safety improvement programmes, such as the Safer Patients Initiative and Safer Clinical Systems, the Health Foundation knows that safety is the product of complex interactions of attitudes, behaviours and resources. Examining a single element in isolation can lead to false assurance of safety. Moving from an approach that largely looks at what we can learn when something goes wrong to one that looks at how we can make sure whole systems go right in the first place will be critical to shifting attention from measuring errors to designing for safety. To do this we need a way of examining how well a healthcare system is designed to guarantee safety.

As this report demonstrates, other safety-critical industries have responded to their own inquiries into safety failures by the development of 'safety cases'. For example, the inquiry into the explosion of the Piper Alpha offshore oil production platform in the North Sea in 1988 led to the Offshore Installations (Safety Case) Regulations 2005, which require petrochemical installations to proactively assess potential risks and so design systems to reliably prevent them from being realised.

* Department of Health. *An Organisation with a memory*. The Stationery Office, 2000.

† The Health Foundation. *How safe are clinical systems?* The Health Foundation, 2011.

This report reviews the available evidence and practice in order to provide a clear description of how safety cases have been used in other safety-critical industries, and to identify and describe their potential application within healthcare.

Safety cases are built around an explicit agreement of the level of safety that is deemed acceptable. Defining what is meant by safety within a particular system is a surprisingly difficult task, but it is essential in order to diagnose the risks inherent in the way the system currently operates. Once risks have been identified, modifications can be put in place to ensure that those risks are reduced or eliminated and the system reliably delivers the expected levels of safety. Safety cases could provide a structured tool for showing that the local risks to clinical systems have been both identified and addressed.

Unlike performance management dashboards, which aggregate and summarise data, safety cases increase the depth of scrutiny by gathering evidence of safety from a range of sources (including risk assessments, incident reporting, human factors analysis and operational experience). Local intelligence is often lost in standardised tools and, in order to avoid this, it is important to include all frontline staff in the production of safety cases, not outsource them to external consultants. By asking healthcare professionals to look at hypothetical scenarios, safety cases can create psychological safety and avoid the potential for blame that can occur when discussing actual incidences of patient harm.

Safety cases are not a replacement for incident reporting. Rather, they are a proactive technique for illuminating the important, but often invisible, risks in clinical systems, increasing the reliability of the system and so reducing adverse events. The evidence gathered to support the safety case is used to argue that risks within the system have been identified and managed so that the desired levels of safety are reliably achieved.

Arguably, the real value of safety cases may come from the process of developing them rather than the end product. Governance committees and boards, as well as clinical teams, can learn as much from the way a safety case argument is developed as from the data itself. Safety cases provide a means of promoting structured thinking about risk that facilitates a consensus between managers and healthcare staff. By making explicit the assumptions about what constitutes safety, safety cases provide a rich learning tool that can enhance the learning culture of an organisation and encourage all staff to constantly scan the environment for potential risks to safety.

The Health Foundation is exploring the development of safety cases in healthcare through our Safer Clinical Systems programme. Eight healthcare organisations are testing how clinically relevant and meaningful safety cases can improve the management of safety across different clinical settings. The learning from this work could have far-reaching implications, not just for how staff assure safety within their clinical settings, but also for how the regulators and commissioners of healthcare services monitor patient safety in the UK.

Elaine Maxwell
Assistant Director
The Health Foundation

Abbreviations

ALARP – As low as reasonably practicable

ASCE – Assurance and safety case environment

COMAH – Control of major accident hazards regulations

CAE – Claims, argument and evidence

CQC – Care Quality Commission

DSCN – Data set change notice

ETA – Event tree analysis

FDA – Food and Drug Administration (USA)

FMEA – Failure mode and effects analysis

FMECA – Failure mode, effects and criticality analysis

FTA – Fault tree analysis

GSN – Goal structuring notation

HAZOP – Hazard and operability study

HSE – Health and Safety Executive

IEC – International Electrotechnical Commission

ISO – International Organization for Standardization

MAPP – Major accident prevention policy

PCA – Provider compliance assessment

QRP – Quality risk profile

SCR – Safety case regulations

SCS – Safer Clinical Systems

SMS – Safety management system

Executive summary

This report presents the findings of the study, *A pragmatic review of the use of safety cases in industry – lessons and prerequisites for their application in healthcare,* carried out from February to June 2011.

Supplements to this report are available to download from www.health.org.uk/safetycasesreport

The supplements contain:

- details of surveys on the use of safety cases in six safety-critical industries (Supplements A-F)
- a review of the application of safety cases to medical devices (Supplement G)
- a systematic review of published literature for evidence of the purposeful adoption of safety cases in healthcare (Supplement H).

Aims

The aims of the project were to describe safety case use in selected safety-critical industries, to make pragmatic recommendations for the adoption of safety cases in healthcare and to outline possible healthcare application scenarios.

Background

In safety-critical industries, manufacturers and operators of systems have to provide evidence of adequate safety performance of their systems to the respective regulatory authorities. The way this is done has changed significantly over the past 20 years, predominantly in response to major accidents and changes to the economic environment (for example, the privatisation of railways leading to a fragmented industry and mixed economy). Previously, manufacturers and operators claimed safety through satisfaction of specific standards and technical requirements specified by the regulator. However, this has proven to be an ineffective and inefficient method of safety management. Current approaches require that manufacturers and operators demonstrate that they have adopted a thorough and systematic process to proactively understand the risks associated with their systems and to control these risks appropriately. They still need to demonstrate compliance with any applicable requirements specified by the regulator, but this approach goes beyond the reactive and standards-based approach to safety management.

In the UK, these duties are often fulfilled through the use of safety cases. The purpose of a safety case is to provide a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is acceptably safe for a given application in a given context. The core of the safety case is typically a **risk-based argument and corresponding evidence** to demonstrate that all risks associated with a particular system have been identified, that appropriate risk controls have been put in place, and that there are appropriate processes in place to monitor the effectiveness of the risk controls and the safety performance of the system on an ongoing basis. The use of safety cases is an accepted best practice in UK safety-critical industries and is adopted by companies as a means of providing rigour and structure to their safety management systems.

Project overview

The project aims were realised through three work programmes.

- **Work programme 1 (WP1)** surveyed safety case practices in six safety-critical industries, assessed the main drivers and barriers and made recommendations for the adoption of safety cases in healthcare. The surveys were produced through selective, expert-driven reviews. Safety case use is common in the industries surveyed and reflects a shared understanding of safety and a mature safety culture. Care needs to be taken that the development of safety cases does not become a bureaucratic exercise without actual safety benefit.
- **Work programme 2 (WP2)** provided a description of emerging applications of safety cases in healthcare. A systematic review of the published literature identified three application domains: medical devices, health informatics and health systems. Most literature related to the adoption of safety cases in the medical devices domain, with some publications starting to address the area of networked medical devices and general health informatics applications. Connecting for Health has issued guidance on the development of clinical safety cases for the National Programme for IT. Safety case use for general health systems has not been addressed to any significant extent in the literature thus far. The main drivers for the adoption of safety cases in healthcare appear to be the current standardisation activities promoted by bodies such as the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and the US Food and Drug Administration (FDA). A selective, expert-driven review was conducted specifically for medical devices to provide further insights.
- **Work programme 3 (WP3)** identified possible application scenarios for safety cases in healthcare and suggested corresponding research areas. Central to this is the notion of an operational or clinical safety case: a structured argument constructed from a clinical perspective about why a particular service is safe. Such an approach may lead to greater clinical engagement in the regulatory process by ensuring that the learning derived is clinically relevant and the process is understandable to frontline staff. Safety cases may also facilitate communication between different stakeholders in complex healthcare environments and provide structure to the safety activities of healthcare organisations.

Key lessons

Benefits

A distinguishing feature of all the industries reviewed is the implementation of **highly structured approaches to safety management** to ensure that organisations are proactively identifying, assessing, mitigating and monitoring risk. The safety case regime is a means of establishing a formal structure for these activities and ensuring that a disciplined and standardised approach to managing risk is adopted. In healthcare, safety cases could be a useful tool to promote structured thinking about risk among clinicians, to foster multidisciplinary communication about safety and to enhance clinical engagement in the regulatory process. Further benefits of safety cases identified in the review include the following.

- **Integrating evidence sources**. Safety cases provide a structured means of integrating safety evidence from diverse sources such as trials, human factors analysis, testing and operational experience. They facilitate assessment of the extent to which the assembled set of diverse evidence is comprehensive and complete and whether it covers all identified safety issues.
- **Aiding communication among stakeholders**. Stakeholders in safety-critical systems include diverse actors such as system designers, manufacturers, operators, maintainers, managers, regulators and the public. Safety cases act as a focus for discussion between these stakeholders by allowing critical review of the beliefs and evidence as to why a system is acceptably safe. Stakeholders can provide input and raise concerns, and they can query the resulting safety case to see how their issues have been addressed.

- **Making the implicit explicit**. The act of establishing and documenting a safety case helps expose existing implicit assumptions and risk acceptance judgements. Having documented a case, it becomes easier to review the arguments, question the evidence and challenge the adequacy of the approach presented. This creates greater transparency in the overall process.
- **Aiding safety management and governance**. Safety cases ensure that appropriate safety evidence is presented and they may reduce the risk of safety issues 'falling down the cracks'. Safety cases further allow targeting of resources and efforts, thus avoiding spending wildly varying and disproportionate amounts of effort on risk management.

Risks and challenges

The review also provided insights into interrelated challenges that the industries have faced that need to be addressed in healthcare when considering the adoption of safety cases. The challenges identified include the following.

- **Becoming a paper exercise.** Safety cases must not become just another 'filed return'. The production of a safety case is an opportunity for gaining greater understanding of the current picture of safety and potentially making safety improvements.
- **Being removed from everyday practice.** Safety cases are supposed to address the realities of everyday system operation. It is important that they do not become a desk exercise that relates only dimly to actual practice. The primary concern of a safety case should lie in demonstrating safety, rather than being an exercise in attempting to shift liability, or in merely demonstrating compliance with 'due practice'.
- **Being produced by the wrong people.** Organisations may be tempted to outsource the production of safety cases to external consultants. This would defeat the purpose of a safety case of ensuring that organisations themselves consider the risks associated with their systems in a systematic and thorough way. Safety case development needs to involve all the relevant stakeholders with an understanding of, and involvement in, what actually makes systems safe (or unsafe).

Recommendations

Safety cases have the potential to support healthcare organisations in the implementation of structured and transparent systems for patient safety management. Such structured approaches have proved to be effective and indispensable tools in safety-critical industries. The adoption of safety cases needs to be accompanied by appropriate guidance and training as well as a continuing development of safety culture maturity.

The benefits of the adoption of safety cases need to be demonstrated in targeted case studies and pilots. This may probably be achieved more easily in areas where there are recognised patient safety risks or where there has already been some interest in the adoption of systematic and structured approaches to safety assurance, such as in the area of medical devices. However, there is also a need to investigate the applicability and utility of safety cases on the health system level – for example, through the use of hierarchies of safety cases. The use of safety cases as a regulatory instrument to facilitate the regulatory process and ensure that feedback provided to organisations is clinically relevant should be investigated in collaboration with the regulator.

Chapter 1:

Project overview

A distinguishing feature of safety-critical industries is the implementation of **highly structured approaches to safety management** to ensure that organisations are proactively identifying, assessing, mitigating and monitoring risk. These lessons have been learned following major industrial accidents and this is accepted best practice across industries. The safety case regime is an accepted means of establishing a formal structure for these activities and ensuring that a disciplined and standardised approach to managing risk is adopted. In healthcare, safety cases could be a useful tool to promote structured thinking about risk among clinicians, to foster multidisciplinary communication about safety and to enhance clinical engagement in the regulatory process.

The purpose of a safety case (also, more generically, known as an assurance case) can be defined as communicating a clear, comprehensive and defensible argument that a system is acceptably safe to operate in a particular context. In addition, a safety case is a valuable tool for bringing about a systematic approach to safety and for providing a record of management's commitment to safety. In many UK safety-critical industries, the use of safety cases is a regulatory requirement. In healthcare, there have been first attempts at adopting the safety case concept for medical devices, promoted by the US Food and Drug Administration (FDA).

Within the Health Foundation's Safer Clinical Systems (SCS) programme, the safety case concept has been introduced as a way of structuring thinking around patient safety and as a means of integrating different sources of evidence (both quantitative and qualitative).

This report presents the results of a study that reviewed the use of safety cases in six safety-critical industries, as well as emerging use of safety cases in healthcare, in order to identify lessons and prerequisites for the more widespread and systematic application of safety cases in healthcare.

Aims

The aims of this study were to provide:

- a clear description of safety case use in selected safety-critical industries
- pragmatic recommendations for the adoption of safety cases in healthcare
- outlines of possible healthcare application scenarios.

Methods

The project entailed a review element to provide evidence, as well as a development element to work up practical examples.

Experts conducted short reviews of the literature and current safety case practices in six safety-critical industries to describe the use of safety cases in the respective industry and to identify any lessons relevant to the adoption of the safety case concept in healthcare. These narrative surveys, which are available as supplements to this report (see www.health.org.uk/safetycasesreport), follow a shared overall structure describing the regulatory context and best practices in the respective industry, the developments and drivers that led to the adoption of the safety case regime, the types of safety cases and their content, as well as recommendations for healthcare.

A systematic review of the published literature relating to the use of safety cases in healthcare was undertaken to identify and describe first experiences with the safety case concept in healthcare. A short expert-driven review of recent efforts and developments around international standards provided further insights into the application of safety cases for medical devices.

Outline application scenarios were produced with the clinical input of volunteers who participated in a project workshop.

Report overview

This report provides a short introduction to safety cases (Chapter 2) and presents the findings of the three project work programmes.

- **Work programme 1 (WP1)** surveyed safety case practices in six safety-critical industries, assessed the main drivers and barriers and made recommendations for the adoption of safety cases in healthcare. (Chapter 3)
- **Work programme 2 (WP2)** provided a description of emerging applications of safety cases in healthcare. (Chapter 4)
- **Work programme 3 (WP3)** identified possible application scenarios for safety cases in healthcare and suggested corresponding research areas. (Chapter 5)

The report briefly discusses potential benefits and risks of using safety cases in healthcare, as well as issues deserving further investigation. (Chapter 6)

Supplements to the report contain details of the reviews undertaken in work programmes 1 and 2. Visit www.health.org.uk/safetycasesreport to download the supplements.

Chapter 2:

An introduction to safety cases

Background

The development and operation of systems such as nuclear power plants, petrochemical plants, aircraft and modern defence systems entail significant risks to people and the environment. The Deepwater Horizon explosion and subsequent oil spill in 2010 and the 2011 Fukushima nuclear incident are only two of the accidents and disasters that are regular reminders of these risks.

In safety-critical industries, manufacturers and operators of systems have to provide evidence of adequate safety performance of their systems to the respective regulatory authorities. The way this is done has changed significantly over the past 20 years, predominantly in response to major accidents and changes to the economic environment (for example, the privatisation of railways leading to a fragmented industry and mixed economy). Previously, manufacturers and operators claimed safety through satisfaction of specific standards and technical requirements specified by the regulator. However, this has proved to be an ineffective and inefficient way of safety management. On the one hand, this approach prompted a practice of 'tick-box' safety management, where the focus was too much on compliance with standards and regulations rather than on understanding of risks. On the other hand, the approach also proved to be too restrictive, hindering progress in industries that are driven by technological innovations. Often, standards became quickly outdated and overtaken by advances in technology.

As a result, current approaches require manufacturers and operators to demonstrate that they have adopted a thorough and systematic process to proactively understand the risks associated with their systems and control these risks appropriately. They still need to demonstrate compliance with any applicable requirements specified by the regulator, but this approach goes beyond the reactive and standards-based approach to safety management.

In the UK, these duties are often fulfilled through the use of safety cases. The purpose of a safety case is to provide a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is acceptably safe for a given application in a given context.[1] The core of the safety case is typically a **risk-based argument and corresponding evidence** to demonstrate that all risks associated with a particular system have been identified, that appropriate risk controls have been put in place, and that there are appropriate processes in place to monitor the effectiveness of the risk controls and the safety performance of the system on an ongoing basis. The use of safety cases is an accepted best practice in UK safety-critical industries and is adopted by companies as a means of providing rigour and structure to their safety management systems. This is in line with recommendations made by Lord Cullen in the highly influential public inquiry into the Piper Alpha oil platform explosion.[2] Lord Cullen's report emphasises that meeting regulatory requirements should only be a secondary function of the safety case – its primary function is to provide assurance to the operators of safety-critical systems **themselves** that they have followed a systematic and thorough approach to ensure that their systems are safe.

Benefits

A distinguishing feature of safety-critical industries is the implementation of **highly structured approaches to safety management** to ensure that organisations are proactively identifying, assessing, mitigating and monitoring risk. The safety case regime is a means of establishing a formal structure for these activities and ensuring that a disciplined and standardised approach to managing risk is adopted. In healthcare, safety cases could be a useful tool to promote structured thinking about risk among clinicians, to foster multidisciplinary communication about safety and to enhance clinical engagement in the regulatory process. Further benefits of safety cases identified in the review include the following.

- **Integrating evidence sources.** Safety cases provide a structured means of integrating safety evidence from diverse sources, such as trials, human factors analysis, testing and operational experience. They facilitate assessment of the extent to which the assembled set of diverse evidence is comprehensive and complete and whether it covers all identified safety issues.
- **Aiding communication among stakeholders.** Stakeholders in safety-critical systems include diverse actors such as system designers, manufacturers, operators, maintainers, managers, regulators and the public. Safety cases act as a focus for discussion between these stakeholders by allowing critical review of the beliefs and evidence as to why a system is acceptably safe. Stakeholders can provide input and raise concerns, and they can query the resulting safety case to see how their issues have been addressed.
- **Making the implicit explicit.** The act of establishing and documenting a safety case helps expose existing implicit assumptions and risk acceptance judgements. Having documented a case, it becomes easier to review the arguments, question the evidence and challenge the adequacy of the approach presented. This creates greater transparency in the overall process.
- **Aiding safety management and governance.** Safety cases ensure that appropriate safety evidence is presented and reduce the risk of safety issues 'falling down the cracks'. Safety cases further allow targeting of resources and efforts, thus avoiding spending wildly varying and disproportionate amounts of effort on risk management.

Risks and challenges

Every industry is subject to diverse pressures and influences arising from different priorities such as cost-effectiveness, but also safety. In the absence of serious adverse outcomes that serve as constant 'reminders' of the risks associated with systems in safety-critical industries, there is the danger that resources dedicated to safety management may be deployed for other priorities and that plausible shortcuts are adopted that may result in more dangerous practices. Challenges related to the adoption of safety cases that need to be overcome include the following.

- **Becoming a paper exercise.** Safety cases must not become just another 'filed return'. The production of a safety case is an opportunity for gaining greater understanding of the current picture of safety and for potentially making safety improvements.
- **Being removed from everyday practice.** Safety cases are supposed to address the realities of everyday system operation. It is important that they do not become a desk exercise that relates only dimly to actual practice. The primary concern of a safety case should lie in demonstrating safety, rather than being an exercise in attempting to shift liability, or in merely demonstrating compliance with 'due practice'.
- **Being produced by the wrong people.** Organisations may be tempted to outsource the production of safety cases to external consultants. This would defeat the purpose of a safety case of ensuring that organisations themselves consider the risks associated with their systems in a systematic and thorough way. Safety case development needs to involve all the relevant stakeholders with an understanding of, and involvement in, what actually makes systems safe (or unsafe).

Content of a safety case

As mentioned above, the core of a safety case is typically a risk-based argument and corresponding evidence. The aim is to provide assurance that all risks associated with a particular system have been identified, that appropriate risk controls have been put in place and that there are appropriate processes in place to monitor the effectiveness of the risk controls and the safety performance of the system on an ongoing basis.

Structurally, a safety case consists of three key elements: claims, arguments and evidence. Claims define clearly the safety objectives that are to be achieved. The safety argument communicates explicitly how the safety evidence relates to and satisfies claims about a system's safety. All these elements are crucial, since evidence without a proper argument is unexplained and an argument without sound evidence is unfounded.[3]

The specific structure of the arguments and the types of evidence may vary depending on the industry and the system under consideration. However, in general a safety case should clearly describe the following elements.

- **The system and its operational context.** Safety can usually only be claimed for an assumed set of circumstances and particular applications. It is important that the boundaries of the system under consideration are specified and that the assumed operational context is described.
- **The safety claims and safety criteria.** A frequently encountered claim is that a system is acceptably safe. The notion of acceptability of risk needs to be described and the criteria that the organisation is going to apply to determine acceptability of risk need to be stated.
- **How hazards have been identified and how the risk they pose has been assessed.** Hazardous situations that may contribute to harm need to be proactively identified and the risks they pose need to be determined through a systematic and transparent process. This provides an overview of the risk that is potentially associated with a given system.
- **What kind of risk control measures have been put into place and why they are effective.** Once risks have been identified and assessed, the safety criteria will be applied to determine the need for reduction of particular risks. Hazards posing risks that require further reduction should either be eliminated or, where this is not possible, the risk should be reduced through risk controls that reduce the likelihood of occurrence of the particular hazard or interventions that mitigate the severity of the consequences should the hazard occur. The ways in which the practical effectiveness of the risk controls will be monitored and determined need to be described.
- **Why the residual level of risk is acceptable.** When risk controls have been applied, each hazard will usually carry a residual level of risk. An argument and evidence need to be put forward to demonstrate that the residual risk associated with individual hazards is acceptable and that the overall residual risk of the system is acceptable according to the safety criteria specified previously.
- **Roles, responsibilities, organisational safety policies and organisational safety management system.** An overview needs to be provided of how safety is managed organisationally, who is responsible for particular safety management activities, what kind of resources are made available for safety management and how the information collected about the safety performance of the system is fed back to management and external stakeholders to trigger action where required.

The safety evidence provided to back up claims can be quantitative as well as qualitative, analytical as well as empirical. Common types of evidence include, for example, descriptions of analytical hazard identification and risk assessment processes and their results, measurements and audits of system performance and relevant parameters, investigation reports of incidents and adverse events, action plans and minutes, staff surveys and competency assessments.

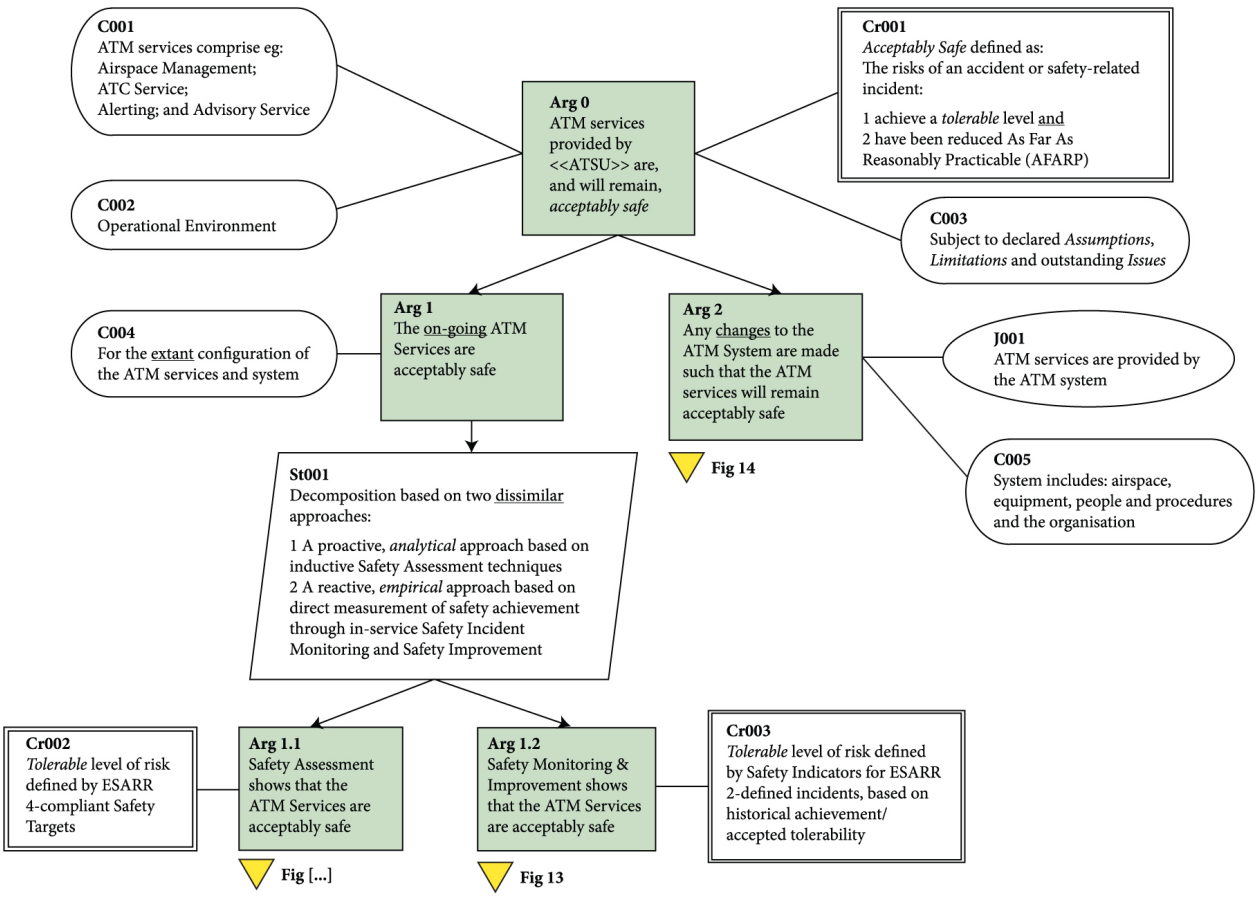
The description given above of the content of a safety case represents safety management activities that any responsible organisation in safety-critical industries is expected to perform. The safety case regime provides structure and transparency to these activities, opens up the safety management activities to review and critique, and allows for an allocation of resources proportional to the risks posed by the system or different aspects of the system.

Communicating the safety case

The safety case is the whole safety justification, including every appropriate piece of evidence.[4] The 'safety case report', on the other hand, is a document that summarises the key elements of the safety case and provides reference to the supporting evidence as appropriate. Often, the safety case report is structured into sections such as in the example above. Safety case reports can become very long, technical and difficult to read and make sense of. In practice, a useful way of making explicit the reasoning and the structure behind the safety case is the use of graphical notations, such as the goal structuring notation (GSN) developed at the University of York. Usually, the core of the argument can be communicated graphically fairly simply and coherently. References can then be included to documents that retain the technical information and can be consulted as required. A goal structure links claims, argument and evidence and shows how claims are successively broken down into sub-claims until they are supported by direct reference to available evidence.[3] GSN is now used widely in different industries and tool-support is available to create and manage complex goal structures (see, for example, www.adelard.com/asce).

An example taken from the EUROCONTROL *Safety Case Development Manual* is provided in Figure 1.[5] It describes a generic high-level argument for assuring the safety of air traffic management services and essentially follows the logic outlined above. The goal structure has a number of contextual elements that serve to describe, for example, the operational environment (C002) and what is meant by 'acceptably safe' (Cr001) – that is, the safety criteria.

Figure 1: Generic high-level argument for demonstrating safety of air traffic management services, articulated in GSN[5]



The top-level claim, that the air traffic management services are safe and will remain safe in the future (Arg 0), is broken down into two sub-claims:

- that the services are safe at present (Arg 1)
- that they will continue to be safe when changes are introduced (Arg 2).

In Figure 1, the argument that the services are safe at present is further broken down into two lines of reasoning:

- an analytical assessment of safety risks (Arg 1.1)
- an empirical monitoring of actual safety achievement (Arg 1.2).

These arguments can be broken down further until the resulting sub-claims can be backed up by direct reference to actual evidence.

The analytical assessment of safety risks (Arg 1.1) would typically claim that all hazards have been identified and that the risks associated with the hazards have been controlled to acceptable levels through the introduction of appropriate risk controls. Evidence to support these claims would come from hazard analysis methods (for example, hazard and operability studies (HAZOPs)) and risk analysis methods such as failure modes, effects and criticality analysis (FMECA), fault tree analysis (FTA) and event tree analysis (ETA).

The empirical safety monitoring argument (Arg 1.2) would claim that operational safety performance is monitored through appropriate processes and that the safety performance is adequate. Evidence could come from measures and audits of safety performance, as well as from reporting and learning systems (for example, incident reporting).

A detailed breakdown of this argument and an in-depth safety case tutorial is presented in the EUROCONTROL *Safety Case Development Manual*.[5] While this is written for an air traffic management audience, the overall reasoning and types of arguments and evidence are instructive for a general audience. Ideally, one could envisage a 'clinical safety case development manual' produced specifically for a healthcare audience in the future.

Summary

In safety-critical industries, it is important that organisations adopt a structured, systematic and transparent approach to safety management. Safety cases are a means of bringing this about and they provide assurance to both the public (via the regulator) and the operators of systems that risks have been properly addressed. Safety cases support operators to structure their safety efforts and to provide sufficient rigour. They promote a proactive approach to safety and they may contribute towards a more mature safety culture.

Summary box 1: Safety cases overview

Why – Provides assurance to operators of systems and the regulator that all relevant safety risks have been addressed systematically and reduced to acceptable levels.

What – A clear, comprehensive and defensible argument that a system is safe to operate.

Benefit – Provides assurance, supports operators in structuring their safety efforts and contributes to proactive safety culture.

Chapter 3:

Review of safety case use in safety-critical industries

Work programme 1 (WP1)

Aims: To review the use of safety cases in selected safety-critical industries and to identify lessons learned.

Methods: Domain experts conducted short reviews of the literature and current safety case practices in six safety-critical industries to describe the use of safety cases in the respective industry and to identify any lessons relevant to the adoption of the safety case concept in healthcare. These narrative surveys follow a shared overall structure describing the regulatory context and best practices in the respective industry, the developments and drivers that led to the adoption of the safety case regime, types of safety cases used and their content, as well as recommendations for healthcare.

Outputs: Description of safety case use in safety-critical industries and lessons learned.

Introduction

The use of safety cases as an explicit demonstration that a particular system is acceptably safe to operate under specific circumstances is common practice in most safety-critical industries. However, safety cases were not adopted across these industries at the same time; rather, each industry followed its own learning trajectory, often triggered by specific accidents or other significant events. The purpose of this work programme was to review and provide a description of these developments across a range of different industries and to identify any lessons relevant to the adoption of the safety case concept in healthcare.

The six industries reviewed were: commercial aviation, automotive, defence, nuclear, petrochemical and railways. The reviews are available in supplements A–F, available to download from www.health.org.uk/safetycasesreport

The notion of risk varies across these industries, from accidents with low probability of occurrence, but potentially catastrophic consequences for humans and the environment (for example, nuclear and petrochemical accidents), to accidents that occur more frequently but that tend to involve a smaller number of individuals (for example, car accidents).

Regulatory context and best practice

Manufacturers and operators of systems in the industries included in this review are subject to regulation by national and international bodies that require demonstration of compliance with accepted best practices as documented in relevant standards. For example, UK offshore petrochemical installations are subject to the Safety Case Regulations (SCR);[6] onshore facilities are covered by the Control of Major Accident Hazards Regulations (COMAH).[7] The regulator in both instances is the Health and Safety Executive (HSE). The HSE Nuclear Directorate oversees nuclear operations in the UK; operators of nuclear facilities have to demonstrate compliance with the HSE Safety Assessment Principles[8] as well as a number of international standards. In the UK railways industry, the competent authority (CA) responsible for the enforcement of the Railway

(Safety Case) Regulations[9] was Her Majesty's Railway Inspectorate (HMRI); previously a separate agency, this became part of the Health and Safety Executive in 1993. HMRI was transferred to the Office of the Rail Regulator (ORR) in April 2006, concurrently with the new legislation implementing the European Railway Safety Directive.[10]

A common trend across the industries is that manufacturers and operators of systems need to demonstrate the absence of unreasonable risks. In the UK this is often expressed through the ALARP principle, which requires that all risks be **A**s **L**ow **A**s **R**easonably **P**racticable. This implies that manufacturers and operators are required to make a case for this proactively, rather than through compliance with detailed technical regulations designed reactively to prevent certain accidents from recurring. For example, in the petrochemical industry, the predictive elements of a COMAH safety report (safety case report) should demonstrate that measures have been taken to reduce the likelihood of hazards, and to mitigate their consequences, until the associated risks are ALARP. The HSE's *Safety Report Assessment Manual*[11] states:

> *If all reasonably practicable measures are in place, and the risks are tolerable, then there is nothing more to be done – Individual Risk and Societal Concern must be ALARP.*

The Ministry of Defence's internal requirements for the production of safety cases for ships and ship systems are similar:

> *Safety Cases are required for all new ships and equipment as a means of formally documenting the adequate control of Risk and demonstrating that levels of risk achieved are As Low As Reasonably Practicable (ALARP).*[12]

Development and drivers

The history of safety cases and safety case legislation in high-risk industries has been closely linked to the occurrence of high-profile accidents. For example, in the petrochemical industry, major changes were introduced following the 1976 Seveso accident at a small chemical manufacturing facility in Italy and the explosion of the Piper Alpha offshore platform in the North Sea in 1988. Similarly, in the nuclear domain, the incidents at Three Mile Island in 1979 and Chernobyl in 1986 had a major impact on relevant legislation.

In addition, each industry was subject to significant changes within the industry that were then reflected in the approach taken to ensure continuing safety of the systems operated. For example, in the UK the privatisation of British Rail was a major driver for the adoption of safety cases. Both in railways and in aviation, the issue of interoperability across national boundaries was an important influence on relevant legislation and practices. In aviation, the adoption of safety cases was engendered by the technical complexity of the systems under scrutiny, which would prevent any form of external independent oversight if not organised according to a clear structure. Technical complexity of electronic installations in modern vehicles may also have been one of the drivers behind recent developments in the automotive industry that resulted in the development of an international standard for functional safety of road vehicles.[13] Table 1 summarises some of these events and the resulting changes that were introduced.

Table 1: Brief chronological summary of significant events and resulting changes in safety regulations for the petrochemical, nuclear and railway industries

Date	Event	Notes and relationship to safety case requirements
1957	Windscale fire (nuclear)	Graphite core of a nuclear reactor at Windscale, Cumberland (now Sellafield, Cumbria) caught fire, releasing substantial amounts of radioactive contamination into the surrounding area.
1959	Establishment of the Nuclear Installations Act (nuclear)	Required that the civil nuclear power stations would be licensed by the newly formed Nuclear Installations Inspectorate (NII).
1976	Seveso accident (petrochemical)	An uncontrolled exothermic reaction resulted in the release of a dense vapour cloud containing poisonous and carcinogenic dioxin. Ten square miles of land were contaminated, more than 600 people were evacuated and 2,000 treated for poisoning.
1979	Three Mile Island accident (nuclear)	Partial core meltdown in Unit 2 of the Three Mile Island Nuclear Generating Station in Dauphin County, Pennsylvania, USA.
1982	Seveso Directive is adopted (petrochemical)	Council Directive 82/501/EEC on the major accident hazards of certain industrial activities – the so-called Seveso Directive – is adopted. Required substances to be identified and processes described. No requirement to include major accident prevention policy (MAPP) or safety management system (SMS).
1983–1985	Public inquiry into Sizewell B reactor (nuclear)	Long-running review into the acceptability of a novel kind of reactor prior to construction. The review was based on the *Pre-Construction Safety Case.*
1984	Bhopal disaster (petrochemical)	A leak of gas and other chemicals from a plant in India resulted in the exposure of hundreds of thousands of people. Estimates on the death toll varied from 2,000 to as many as 15,000 people. Gave rise to an increased focus on safety culture.
1984	Control of Industrial Major Accident Hazards (CIMAH) Regulations adopted in UK for onshore facilities (petrochemical)	Superseded by COMAH Regulations in 1999. Similar to Seveso I requirements with an emphasis on description.
1986	Chernobyl accident (nuclear)	Reactor vessel rupture and a series of explosions that followed resulted in the deaths of 30 power plant employees and firemen. It also brought about the evacuation of about 116,000 people from areas surrounding the reactor during 1986.
1987	King's Cross Station Fire (London Underground) – 31 deaths (railways)	Radical reform of management on the Underground, including the introduction of a safety management system (SMS) and the first system-wide quantified risk assessment (by 1991).

Date	Event	Notes and relationship to safety case requirements
1988	Clapham derailment – 35 deaths (railways)	Major reforms within British Rail reflecting the response to King's Cross on London Underground.
1988	Piper Alpha disaster (petrochemical)	An oil platform that was later converted to gas production. An explosion on the platform and the resulting fire killed 167 men with only 59 survivors.
1992	Safety Case Regulations (SCR) adopted for UK offshore industry (petrochemical)	The publication in 1990 of Lord Cullen's report into the Piper Alpha disaster paved the way for the introduction of formal safety case requirements in the UK offshore industry.
1992	UK government white paper announcing formal proposals for the privatisation of British Rail (railways)	The principal driver for the subsequent safety case regime.
1994	Privatisation of British Rail and enactment of the Railways (Safety Case) Regulations, 1994 (railways)	First introduction of a mandatory safety case regime in the UK.
1996	Seveso II Directive is adopted (petrochemical)	Implemented in the UK as the COMAH Regulations (see below).
1997	Southall collision – seven deaths (railways)	Signal operated by the infrastructure controller passed at danger by a driver employed by a train operating company.
1999	Ladbroke Grove collision and fire – 31 deaths (railways)	Also a signal passed at danger (SPAD) incident. Southall and Ladbroke Grove accidents led directly to (*inter alia*) a review of the safety case regime.
1999	Control of Major Accident Hazards (COMAH) Regulations adopted in UK for onshore facilities (petrochemical)	Replaced the CIMAH Regulations and introduced a greater degree of uniformity with the offshore SCR. The regulations brought a number of smaller sites under the legislation and introduced a number of new features, including the MAPP and SMS requirements. Also brought an increased emphasis on demonstration rather than description.
2000	Enactment of Railways (Safety Case) Regulations 2000 and 2001 amendments, revising the Safety Case regime (railways)	New regulations directly reflect the analysis and recommendations of the inquiries into Southall and Ladbroke Grove.
2003	Revision of Seveso II Directive (petrochemical)	Revision of Seveso II Directive to include additional requirements for risk assessment. The most important extensions of the scope cover risks arising from storage and processing activities in mining, from pyrotechnic and explosive substances, and from the storage of ammonium nitrate and ammonium nitrate-based fertilisers.

Types of safety cases and content

Across the industries, the purpose of a safety case is similar – namely to provide confidence to both the operators of safety-critical systems and to the regulator, and hence the public, that systems are acceptably safe to operate. In aviation, EUROCONTROL guidance expresses this as:

> *Broadly, the Safety Case is the documented assurance (i.e. argument and supporting evidence) of the achievement and maintenance of safety. It is primarily the means by which those who are accountable for service provision or projects assure themselves that those services or projects are delivering (or will deliver), and will continue to deliver, an acceptable level of safety.*[5]

The specific structure and content of safety cases varies from industry to industry. However, there are several key elements common across the industries.

- Description of the system under consideration and the operating context.
- Definition of the acceptability of risk and any safety criteria that need to be met.
- Identification of hazards: demonstration that all foreseeable (major) hazard scenarios have been identified. Common techniques include failure mode and effects analysis (FMEA) and hazard and operability studies (HAZOPs).
- Analysis and assessment of risk: following the identification of hazard scenarios, realistic assessments of the likelihood of their occurrence should be made and a prediction of the possible consequences undertaken, including situations where existing mitigation measures fail. Options for reducing the risk associated with hazards need to be identified, and decisions about which measures need to be implemented to make the risks to people and the environment satisfy the ALARP criteria need to be described. Common techniques for providing evidence include the use of fault tree analysis (FTA) and event tree analysis (ETA).
- Safety management: operators also need to demonstrate that they have an effective safety management system (SMS) in place. The SMS often encompasses activities such as failure analysis, incident investigation and analysis, and the monitoring of staff competencies.
- Description of roles, responsibilities and organisational safety policy.

Lessons and recommendations for healthcare

In the industries reviewed, the approach to safety and the regulatory environment has evolved in response to technology drivers, market changes, some major accidents and the need for an effective dialogue with a range of stakeholders. While regulation is a key driver, safety cases are not something that is just imposed on the industry by the regulator; rather, they represent a shared approach to how safety should be justified and be seen to be justified. The safety culture in the industries reviewed in this report may be more mature than the current safety culture in healthcare, with patient safety still being a recent and emerging discipline. This may suggest that safety cases should only be adopted in those contexts where there is a good level of safety maturity, both on principles and methods. Otherwise, accompanying actions should be put in place at the same time.

Education and demonstration appear to be key enablers in promoting the safety case concept and hence patient safety. Both regulators and healthcare professionals need to continue to develop their familiarity with systematic and proactive approaches to engineering safe clinical systems. Demonstration, in the form of healthcare-specific case studies and pilot applications, is important to convince the community of the value of a safety case. In particular, these case studies and pilot applications should show why and how a safety case adds value to the overall safety process.

Safety cases can be fruitfully applied to develop systematic and structured safety activities. This will bring immediate benefit to those preparing the safety case. As mentioned above, a key aim of safety case development is to provide assurance to the organisation that it has thoroughly and systematically considered all relevant safety issues.

A well-organised process may be the basis for effective coordination among service providers, manufacturers of systems and the regulator. The complexity of modern industrial systems is such that collaboration between different organisations cannot be avoided in the delivery of any substantial service, and systems for communication and sharing of data become essential. The same applies to healthcare, where inter-disciplinary and inter-organisational collaboration in the provision of care is the norm, supported by a multitude of medical devices and other health products. The adoption of safety cases may ensure that resource is committed to the necessary degree of cooperation at all levels.

In all the industries reviewed, there is a concern that the adoption of safety cases could result in bureaucratic overheads and meaningless paper exercises. In addition, training requirements on the part of the regulator and the manufacturers and operators of systems have often been underestimated. For example, the review following the loss of a Nimrod aircraft in Afghanistan in 2006 warns that the safety case regime adopted in the defence sector has led to a culture of 'paper safety' at the expense of real safety.[14] It acknowledges the importance of safety cases in principle but makes a range of recommendations to facilitate their effective adoption in practice. In a healthcare setting, it is therefore vitally important to construct safety cases that are relevant to clinical practice, ideally driven by frontline clinicians.

Summary box 2: Lessons for healthcare from safety case use in other industries

Regulation – Regulation is a main driver behind the adoption of safety cases.

Education – Education and demonstration are key enablers**.**

Clinical relevance – Clinical relevance and engagement by clinicians are crucial prerequisites for avoiding a bureaucratic approach to safety management.

Chapter 4:

Review of current safety case use in healthcare

Work programme 2 (WP2)

Aims: To identify and describe first experiences with current use of safety cases in the area of medical devices as well as any other healthcare domain.

Methods: Systematic literature review; expert-driven review; expert consultation.

Outputs: Appraisal of any evidence of safety case use in healthcare and discussion of lessons and challenges.

Introduction

In the safety-critical industries reviewed for this project, the development and maintenance of safety cases are regulatory requirements and accepted best practice. Currently, no such explicit regulatory requirement exists in healthcare. The aims of this work programme were to identify and describe emerging applications of safety cases within different areas of healthcare. To this end, a pragmatic expert-driven review of recent developments in the use of safety cases (assurance cases) for medical devices was conducted, as well as a systematic review of the published literature for evidence of the purposeful application of the safety case concept within healthcare. This work was done from January to March 2011.

Methods

The expert-driven review of the application of safety cases to medical devices was carried out by Adelard, based on their experiences of working in this area. The full review can be found in Supplement G.

The systematic review of the published literature across all healthcare domains was carried out by Mark-Alexander Sujan of Warwick Medical School. Full details of the systematic review can be found in Supplement H.

See www.health.org.uk/safetycasesreport to download these supplements.

Results

The systematic literature search identified 16 papers for inclusion in the review. In addition, a selection of relevant standards were reviewed: ISO 14971, IEC 60601-1, IEC 80001-1, DSCN 14/2009, DSCN 18/2009 and the Care Quality Commission (CQC) Essential Standards of Quality and Safety.

Three broad application domains were identified and the papers grouped accordingly.

– **Medical devices.** As medical devices increasingly contain programmable elements that make them more flexible, adaptable and allow greater interconnectivity, the assurance that safety objectives are met and the certification of medical devices are also becoming more difficult. This has given rise to new developments reflected in standards and guidance issued by bodies such as the FDA[15] and ISO.[16] In order to react to the significant rise in the number of problems reported with the use of infusion pumps, the FDA has taken up the assurance case approach as part of the pre-market notification submission. The FDA is also proposing that manufacturers take a goal-based approach in their assurance cases, preferably using the claims-arguments-

evidence (CAE) paradigm or goal structuring notation (GSN). The design and implementation of such programmable medical devices may benefit from methods and techniques developed within the software and engineering communities for the development of safety-critical computer-based systems, including the use of safety cases.

- **Health informatics.** Within healthcare, there are also an increasing number of health informatics products that are not strictly speaking medical devices, but which may still present risks to the patient. In the UK, Connecting for Health has issued guidance about the development of clinical safety cases to manufacturers of health informatics systems and organisations that use these products.[17,18] This was in response to the perception that the National Programme for IT was not addressing safety in a structured and proactive manner. Connecting for Health reports positive experiences with the safety case approach, but points out that education and support are vital and that there are still problems with the uptake by manufacturers.[19] A similar approach is followed in the recent standard IEC 80001-1, which deals with networks of medical devices.[20]
- **Health systems.** Finally, as the discipline of patient safety matures and organisations are gaining experiences and expertise in the application of systematic methods for identifying and managing risks to patient safety, the use of safety cases or structured safety arguments may be a useful way of documenting and guiding an organisation's safety efforts. Only one position paper was identified in this category.[21] This is not surprising, since the safety case concept has been developed within the engineering communities and is traditionally applied to hardware and software products first. As the safety case concept takes hold in the domains of medical devices and health informatics applications, we may expect to see more work in this category of general health systems in the future.

Discussion

The systematic literature review demonstrated that research on, and application of, safety cases to healthcare is scarce. The majority of papers identified described different aspects relating to safety assurance of medical devices. Within the standardisation community there is currently a lively debate around these issues and it appears that developments are driven by these efforts. This extends to aspects of networked medical devices, where a key standard is the main focus and driver for developments in this direction (IEC 80001). It is not clear to what extent manufacturers of medical devices are actively supporting the adoption of the safety case concept.

There were also some examples where the safety case concept has been applied to the wider health informatics field; Connecting for Health is leading in this domain. Unfortunately, despite encouraging findings, there appears to be little awareness of these developments within the wider health informatics or patient safety community.

Apart from a position paper, there is no evidence that safety cases have been applied to the wider health system where the focus has not been on the introduction of technology.

The reviews carried out as part of this work programme suggest that the main drivers for developments currently are the standardisation efforts of organisations such as the FDA. This appears to be an important factor in securing the attention of the industry. The literature reviews further suggest that healthcare organisations need to take greater responsibility for actively compiling evidence that the complex systems they operate to provide patient care are, in fact, safe. This, however, will only be possible when adequate resources and training opportunities are provided to these organisations to enable them to build up the required capability. As can be seen with the FDA and its efforts, training needs for regulators and manufacturers must also be met in the form of expert input, technical guidance documentation and appropriate tool support.

Summary box 3: Current safety case use in healthcare

Medical devices – The FDA is recommending the adoption of assurance cases as part of the pre-market notification submission for infusion pumps.

Health informatics – Connecting for Health has issued guidance on the preparation of a clinical safety case for health informatics products.

Education – Education and training need to be provided to the organisations producing safety cases as well as the bodies reviewing them.

Chapter 5:

Application scenario and research directions

Work programme 3 (WP3)

As part of the project, a workshop was held with stakeholders from the healthcare community in order to discuss opportunities and challenges for the adoption of safety cases.[22] The next sections summarise the following promising directions for further development and investigation that were identified.

- Clinical safety cases – an approach to developing a safety argument for infusion devices.
- Regulation – integrating the safety case approach with current regulation as a means to enhance clinical engagement and clinical relevance.
- Safety management systems (SMS) – implementation of structured approaches to safety management.

Clinical safety cases – an application scenario

The notion of clinical safety cases – structured safety arguments from an operational perspective – was identified as a possible tool to support healthcare organisations in structuring their safety activities and efforts, and in providing assurance that they have considered patient safety risks systematically and thoroughly. An important aspect of clinical safety cases is that they are intended to be developed from an operational perspective with close involvement of clinicians and frontline staff.

Application scenario

An appropriate application scenario is that of the process of patient infusion – administration of IV fluids – using infusion devices in a hospital department. The clinical safety case would therefore support the claim:

- ***Patient infusion in department X of hospital Y is acceptably safe.***

We believe that this application scenario is appropriate because it:

- **concerns a safety-critical activity:** the introduction of IV fluids to patients is a standard, yet high-risk activity. Administration of the wrong medication or incorrect dosage can have adverse consequences including death. It is, therefore, sensible to start the consideration of a clinical safety case application scenario from a safety-critical activity
- **involves one or more programmable devices and their operators:** infusion pumps are programmed to administer fluids automatically. In the USA, there is much concern from the regulator of medical devices – the FDA – due to the significant rise in adverse events related to infusion pumps. As such, it has issued guidance for the development of assurance cases for infusion pumps. The FDA guidance would therefore provide input to this scenario. The concern about infusion pumps becomes even greater when we take into account the fact that multiple pumps may be used in conjunction on a single patient

– **has a reasonable level of complexity:** it is important for such an exercise to identify a scenario with reasonable scope and complexity. The process of infusion is a straightforward task; however there are several dependencies on activities carried out in other parts of the hospital, such as diagnosis and prescription, or delivery of medication from the pharmacy. The proposed clinical safety case would aim to define its boundaries and identify dependencies on other elements.

Further details about the application scenario are provided below.

Safety argument

In this section, we use the claims-argument-evidence (CAE) approach to safety argumentation to demonstrate some of the key elements of the safety argument and discuss how they would be developed.

As mentioned above, the top-level claim for this clinical safety case would be:

– ***Patient infusion in department X of hospital Y is acceptably safe.***

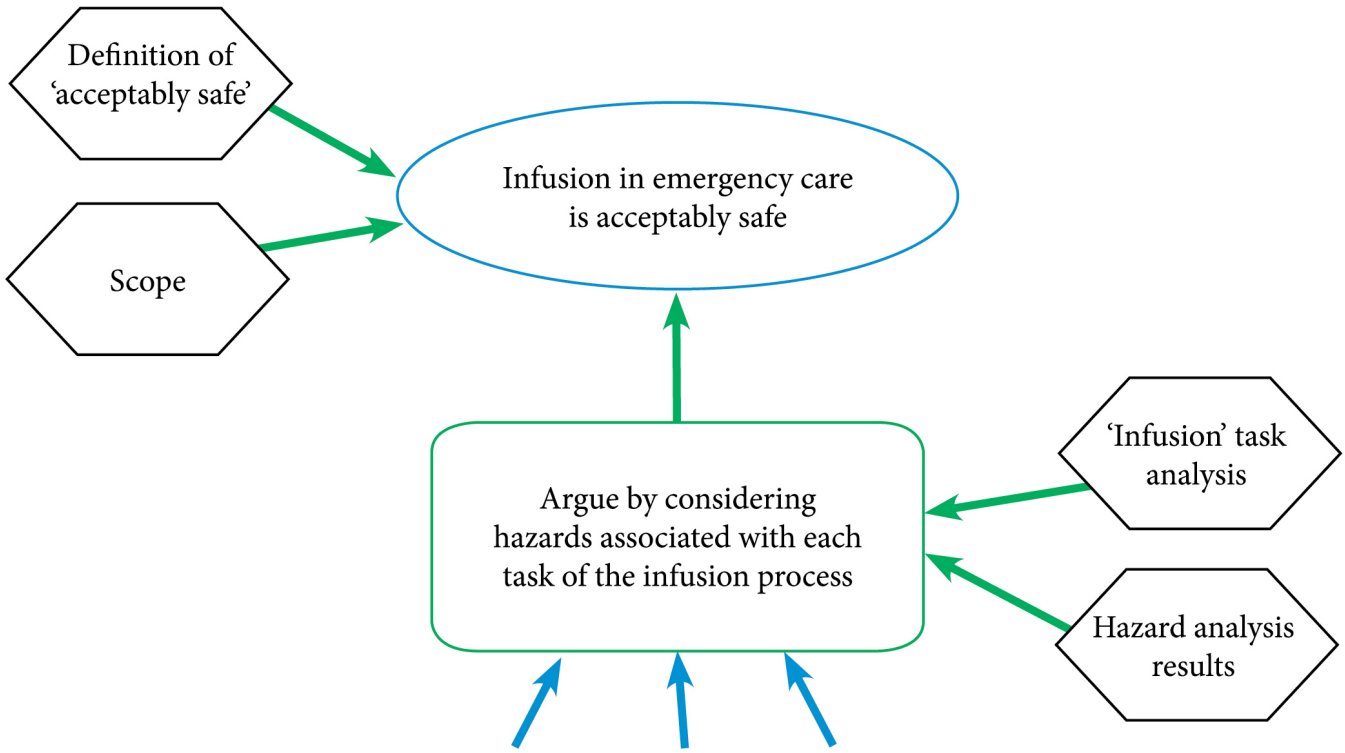
Before proceeding to the safety argument and the evidence, the scope of the clinical safety case needs to be defined. We therefore need to identify and record:

– **the definition of 'acceptably safe':** there should be both qualitative and quantitative elements to this definition, which will draw upon requirements such as legal, contractual, current level of safety and the ALARP principle. This definition will contain risk categorisation and criteria for tolerability of risk; however, we expect there will be significant challenges in accomplishing this, as risk from a hazard is patient-specific. A slightly ill patient and a critically ill patient may face different risk severities from the same hazard

– **the scope of the clinical safety case:** the boundaries of the system demonstrated to be safe must be identified. This will be an 'operational' safety case – a case that covers the operation of certain medical devices. As such, it will cover not only these devices, but also aspects such as user competency, adequacy of supporting procedures and interactions with other hospital departments. Another element of the scope definition is time: how long do we argue that this claim remains valid assuming that the operational conditions do not change?

Figure 2 illustrates the top-level claim and the main argument we envisage would support it.

Figure 2: Proposed clinical safety case top-level claim

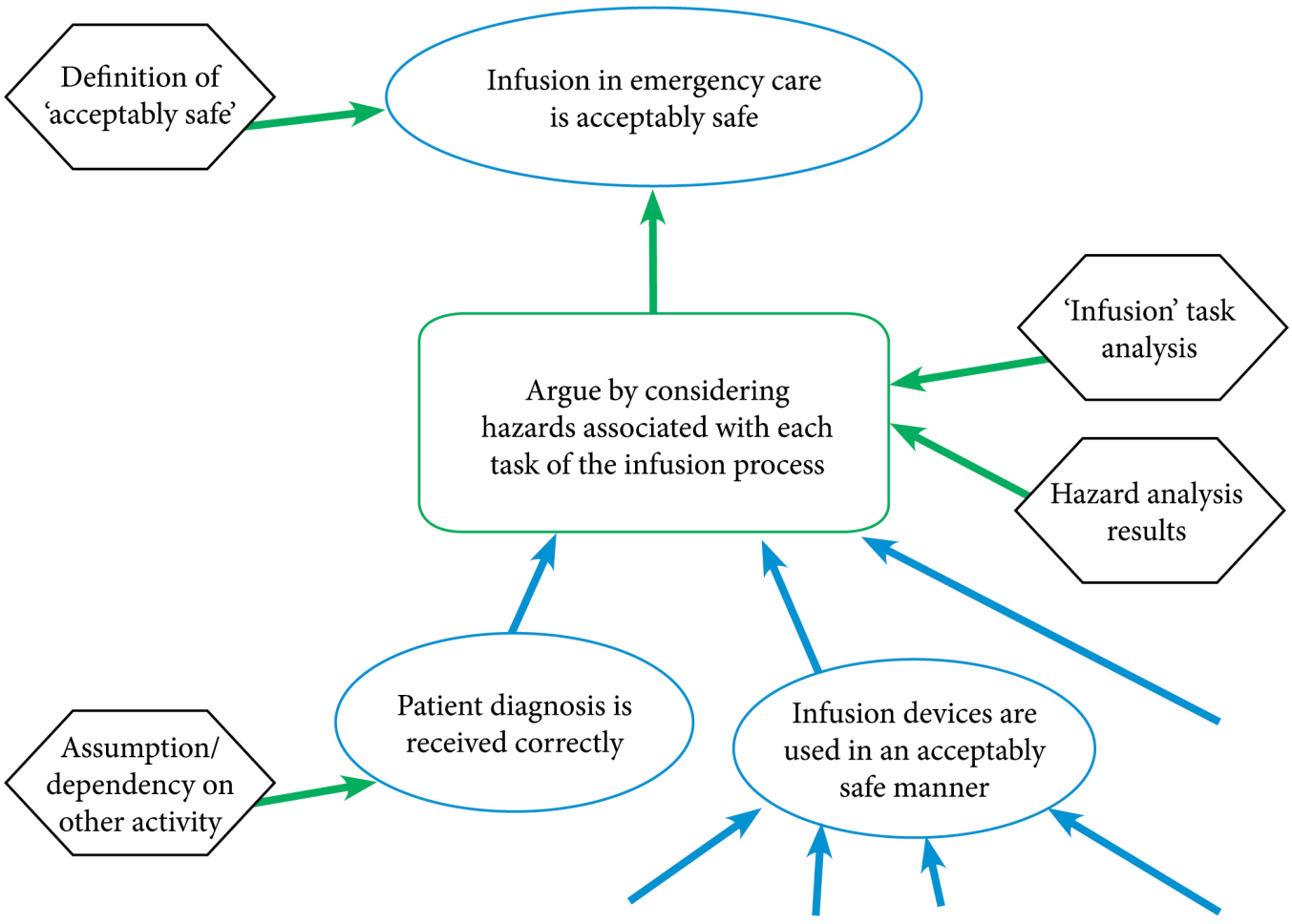


One approach to supporting this claim is to break down the sub-tasks that make up the activity of patient infusion and argue their safety individually. In order to achieve this, we would need to do the following.

- **'Infusion' task analysis:** task analysis is the analysis of how a task is accomplished. This includes a detailed description of both manual and mental activities, task and element durations, task frequency, task allocation, task complexity, environmental conditions, necessary clothing and equipment, and any other unique factors involved in or required for one or more people to perform a given task. Various techniques and tools can be used to carry out and record the results of task analysis. This is important so that all the activities that put together the process of infusion are identified.
- **Hazard analysis:** having conducted a task analysis, we may carry out a hazard and operability study (HAZOP). This is a systematic approach to the identification and evaluation of potential hazards and their mitigations, which is based on the application of a set of guidewords (for example, none, more, less, wrong, other than) on the system. It is important that a HAZOP is multidisciplinary to have comprehensive insight. As such, apart from the safety experts this would involve, for example, a nurse, a physician and a pharmacist.

Figure 3 presents a part of the first level of decomposition as we would expect it. Each of the claims focuses on tasks as defined in the task analysis. The HAZOP will have identified hazards for each of these, so the further levels of decomposition will attempt to demonstrate that each of these hazards are mitigated or controlled until they become 'acceptable'.

Figure 3: Example decomposition of the high-level claim



An important part of this approach is the identification of dependencies on other departments. As we can see from Figure 3, patient diagnosis (and probably drug prescription) is outside the scope of the activity of infusion; however, they are critical inputs. The clinical safety case must identify and record these inputs, as well as any checks and procedures in place to verify them or address potential problems.

Furthermore, claims made should address all states of operation – normal conditions and emergency conditions. The case should also demonstrate not only that infusion is performed safely, but also that infusion does not introduce any additional hazards.

Infusion pumps

It is expected that much of the attention will be on the infusion pump(s) used. Manufacturers' documentation provides detailed instructions on configuration, use and storage of the devices. We would evaluate to what extent these instructions are followed, and what evidence there is for that (for example, logs, evidence of training, procedures), in order to claim that the device is used in the appropriate manner. Any deviations from such practice would have to be adequately justified.

Although the use of individual infusion pumps may be covered by this approach, the situation is different when multiple pumps are used together. Apart from the complexities of the medicines administered to the patient simultaneously, there are also concerns regarding how nurses monitor and use them. There may be issues of alarm management and we expect that procedures should be in place defining how multiple infusion pumps are used at the same time.

Infusion pumps may also be connected to the hospital computer network. Appropriate standards (for example, IEC 80001 – Application of risk management for IT-networks) should be referred to in order to evaluate whether hazards from network connection exist and, if so, if and how they are controlled.

Recommendations: Clinical safety cases

We recommend the following to develop this proposed clinical safety case.

- **Interviews.** Key staff, such as nurses, physicians, pharmacists, medical device manufacturers and hospital IT administrators, would provide input at different stages of the development.
- **Analysis of documents.** Several types of documents, such as manuals for infusion pumps and other devices, hospital procedures, incident reports (if made available), prescription forms etc, will be consulted. Information systems may be examined, and how they are used in the process of infusion (for example, to identify patient records). This, along with interviews, will assist in understanding and documenting the protocols that are followed to carry out patient infusion.
- **Task analysis.** Task analysis is a user-focused approach to the analysis of activities. Various methods exist – for example, hierarchical task analysis – but they all attempt to break down tasks for further analysis. Task analysis is useful because apart from identifying potential error modes, it also identifies information flows and dependencies on other parts of the hospital. The resulting model will be the basis for the hazard analysis.
- **Hazard and operability study (HAZOP).** The HAZOP is crucial. HAZOP is one of the most widely applied hazard identification approaches in the safety-critical domains. A multidisciplinary HAZOP team is likely to provide significant insight, in particular from nurses – not only are they the users, but they also possess tacit knowledge about the process and interact with patients, physicians and others in the hospital to carry out this particular activity.
- **Safety argument development in assurance and safety case environment (ASCE):** ASCE, the Adelard safety case tool, provides a graphical environment for the development of safety cases. The CAE (or GSN) approach in ASCE could be used to develop and report this clinical safety case.

Regulation

Regulation has been identified as a key driver behind the adoption of safety cases. In this section, lessons learned from the regulatory process in other industries are reviewed and recommendations are made for the integration of safety cases with current regulation.

What we can learn from regulation in other industries?

The reviews conducted as part of this project demonstrated that the respective regulators in the different industries adopted the safety case concept across the industries as a means of assuring that safety risks are systematically considered and taken care of. Drivers behind this were serious accidents and incidents which demonstrated that safety risks had not been properly understood, as well as changes to the operating environment, such as privatisation or increasing technological complexity, which necessitated improved communication between increasing numbers of stakeholders.

Safety cases have been adopted as a regulatory instrument in order to:

- contribute to the systematic identification and management of risk
- enhance understanding of organisational safety
- facilitate communication among stakeholders
- simplify the regulatory process and make it easier to understand.

An assessment and critique of regulation in healthcare was not part of the project aims. However, using the experiences and lessons learned from other industries, it is possible to highlight a number of common threats to the efficacy of the regulatory process that may also be present in healthcare. These are that:

- regulation is perceived as a bureaucratic paper exercise, without value to the organisation
- regulation introduces significant overheads in terms of time and resources required
- complex regulatory processes lead to disengagement of frontline staff.

The regulation of healthcare providers in England

Providers of health and adult social care services in England are regulated by the Care Quality Commission (CQC). The CQC has introduced a registration and ongoing monitoring system to ensure that providers are meeting essential standards of quality and safety. The standards are described in the Health and Social Care Act 2008 (Regulated Activities) Regulations 2010 and the Care Quality Commission (Registration) Regulations 2009.

The approach adopted puts the experiences of patients and service users at the centre, specifying outcomes that people can expect of services provided by organisations that comply with the essential standards. In total, there are 28 regulations with associated outcomes. An example relating to equipment is provided in Figure 4.

Figure 4: Outcome 11 associated with Regulation 16 (Safety, availability and suitability of equipment) of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2010

Safety, availability and suitability of equipment

OUTCOME 11

What should people who use services experience?

People who use services and people who work in or visit the premises:

- Are not at risk of harm from unsafe or unsuitable equipment (medical and non-medical equipment, furnishings or fittings).
- Benefit from equipment that is comfortable and meets their needs.

This is because providers who comply with the regulations will:

- Make sure that equipment:
  - is suitable for its purpose
  - is available
  - is properly maintained
  - is used correctly and safely
  - promotes independence
  - is comfortable

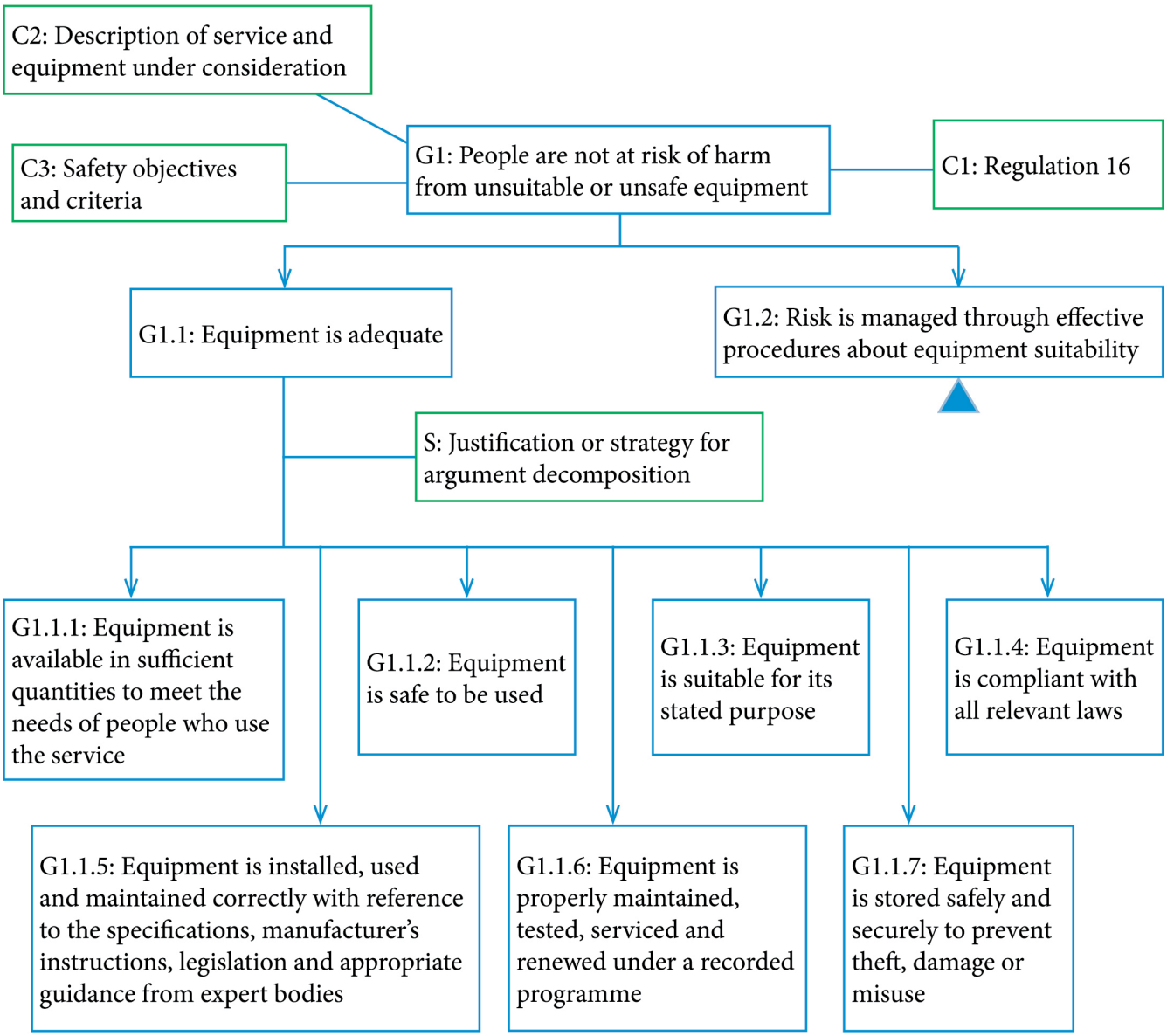
The guidance issued by the CQC includes a number of prompts for each outcome that providers should consider in order to check their compliance. As part of the registration process, providers need to fill in a provider compliance assessment (PCA) form. The PCA asks providers to summarise evidence which demonstrates that they have met the different goals set out in the prompts. The PCA is used in conjunction with a range of other information sources (such as compliance with NHS

Litigation Authority risk management standard in the case of equipment) to produce a quality risk profile (QRP). The QRP is an indicator of the risk of non-compliance with particular regulations. It does not, therefore, indicate whether or not an organisation is safe, but rather serves to focus the attention of the regulator and the provider on particular areas that should be investigated further.

Clinical safety cases as a potential instrument for the regulation of healthcare providers

As mentioned above, the short summary of regulation of healthcare providers in England does not include an assessment or critique of the regulatory process practised by the CQC. As a matter of subjective opinion, the principles behind the process appear very modern and forward thinking. The outcomes and prompts to demonstrate compliance with the regulations could be understood as high-level safety or assurance cases. Figure 5 is a graphical representation of the guidance provided by the CQC for demonstration of compliance with Regulation 16 relating to equipment. A few contextual elements have been added (green) and goal 1.2 has been left undeveloped, but could be developed accordingly from the guidance. Regulation 16 also contains an element relating to the benefits received from use of the equipment, which has been omitted here for simplicity.

Figure 5: Graphical representation of guidance for demonstrating compliance with Regulation 16 (partial representation)



From the guidance, it is not absolutely clear which roles within the provider organisation will compile the evidence intended to demonstrate compliance. Considering the lessons learned from other industries, one of the main threats to successful regulation in healthcare could be the disengagement of clinicians. In such a situation, the evidence would be compiled by management or governance staff and the value and transparency to clinicians may suffer accordingly. Feedback from the CQC to the provider may thus result in 'knee-jerk' fixes imposed on clinicians who may fail to see either the rationale or the value to the service behind such demands.

Recommendations: Regulations

The notion of operational or clinical safety cases, as described above, could be a useful tool to promote structured thinking about risk among clinicians, to foster multidisciplinary communication about safety and to enhance clinical engagement in the regulatory process. Since the CQC approach to regulation already entails a thin or high-level safety argument (albeit not explicitly referred to as such), the development of clinical safety cases would fit well with this kind of thinking. For future study we recommend two actions.

- To investigate, with the regulator (the CQC), bodies with experience in the adoption of the safety case concept (for example, Connecting for Health) and healthcare organisations, whether the adoption of clinical safety cases is feasible as a regulatory instrument to contribute to a transparent regulatory process and to provide meaningful and relevant feedback on a clinical level to healthcare organisations.
- To investigate whether, and through which mechanisms, the development of clinical safety cases leads to greater clinical engagement and a more mature safety culture. This could be a qualitative study intended to explore, through interviews, clinicians' perceptions about the utility of the approach from a clinical perspective, the barriers that need to be overcome to make such an approach practicable, and the effect that participation in pilot studies of clinical safety case development has had on the safety-related attitudes and values of participants, as well as the mechanisms through which any changes in attitudes may have been brought about.

Safety management systems (SMS)

As pointed out earlier, one of the key distinguishing characteristics of safety-critical industries is their structured approach to safety management in order to ensure that risks are proactively identified, analysed, mitigated and monitored. The organisational approach to safety management that defines and implements these activities is usually referred to as the organisation's safety management system (SMS). Every organisation will have an SMS of some sort. In safety-critical industries, an SMS tends to be (ideally) explicitly documented, transparent and proactive. In healthcare, SMSs may not be as proactive or explicitly documented, but healthcare organisations will have rudimentary safety policies and strategies. They will also have some processes for reactive approaches to safety management, such as the review of serious untoward incidents or systems for incident reporting.

There is a close relationship between the SMS and the safety case. The safety case structures the safety activities and explains how the safety evidence relates to the safety claims. It can be used to guide safety activities, to identify where additional safety efforts are required, and to review and critique the organisational approach to safety. The SMS, on the other hand, provides the management structure and the resources for the execution of the safety management activities. These activities, in turn, provide evidence that can be referenced in the safety case to support claims about the system's safety. The development and maintenance of the safety case (as activities) form part of the SMS.

Guidance on the structure of an effective SMS can be derived from most of the domains covered in this review. Some principles for the use of an SMS that may apply to healthcare are described in the following sections.

SMS constituent elements

The SMS should be tailored to each organisation. Organisations differ in type, size and level of safety maturity, not to mention the nature of processes and services being carried out. However, current guidance distinguishes at least the following pillars for an effective SMS.

– Policy and processes.
– Safety achievement.
– Safety assurance.
– Safety promotion.
– Emergency response.

Policy and processes

Every SMS must clearly define policies, procedures, and organisational structures to accomplish its goals, including the allocation of responsibility, authority, and accountability at the proper organisational level.

The safety policy lists all the high-level principles informing the existing safety activities (the 'shall' and 'shall not'). The safety policy reflects the strategic vision and commitment to the values of the organisation, so it should remain relatively stable over time. The policy also informs the creation of new processes.

Safety processes describe the relationships between all stakeholders involved in maintaining safe operations, including the required interfaces, oversight functions and information exchange. Process descriptions can be as simple as a set of instructions, generic guidance, or a complex workflow involving different actors and departments. Regardless of the format, the process should identify who is responsible (the actors involved) for each task, what they receive as input information and what they are supposed to provide as an output.

The safety policy should also cover any applicable legislation, regulations, standards and domain-related best practices.

Safety achievement

The safety achievement pillar includes all the activities dedicated to risk identification and management. The objective of safety achievement activities is to manage risks in order to reduce them, or at least maintain them at an acceptable level, through a continuing process of risk identification, assessment, mitigation and monitoring. It should be noted that safety is achieved by a process, implying constant measurement, evaluation and feedback into the system.

A generic process of risk assessment usually contains the steps:

– system description
– identification of potential hazards
– identification of possible hazard effects
– assessment of hazard effects' severity
– specification of safety objectives
– definition of mitigation actions
– monitoring of the system performance.

Three strategies are typically deployed to manage risks. The strategies are:

– reducing the risk's associated severity
– reducing their frequency
– transferring risks – for instance, to insurance companies.

The three strategies are not mutually exclusive and are often mixed to achieve the best results. In addition to these strategies, certain risks will be **accepted** (in whole or in part) on the basis of acceptance thresholds defined in the **risk acceptance matrix** by combining **frequency** and **severity**.

A variety of techniques exist to support each of the above steps (for example, task analysis, FTA, ETA, FMEA, HAZOP, investigation of incident reports, root cause analysis), with the SMS ensuring an overall framework for their application.

The risk assessment process also applies to the introduction of new elements, or to system changes. Safety achievement activities should be documented in the required format, providing a clear linkage to the organisation's safety policy. The safety case structure can be used to organise such documentation in the safety case report.

Safety assurance

Once policies, processes, assessments and controls are in place, the organisation must incorporate regular management review to assure safety goals are being achieved. This means that the organisation must provide documented assurance that an acceptable level of safety is being met and will be met in the future.

Safety assurance uses a variety of information sources, including:

- safety surveys, audits, inspections and quality assurance activities
- monitoring of safety performance, in order to detect changes in systems or operations which may suggest any element is approaching a point at which acceptable standards of safety can no longer be met, so that corrective action is taken
- incident reporting and systems for organisational learning to monitor and verify the achieved safety levels.

A key concept within an SMS is that these various oversight systems should feed into a system of management review.

Safety promotion

Safety promotion refers to the continuous promotion of safety as a core value in the organisation.

Typical activities include the **dissemination of lessons learned** and the active involvement of operators and staff in a proactive learning process, to foster the bottom-up identification and management of safety issues (safety improvement).

Emergency response

Being able to provide adequate response to emergencies is an integral part of the SMS. The risk to be mitigated is not what led to the emergency, but rather the risk associated with handling the emergency itself. The purpose of emergency response plans (in aviation) is to ensure:

- orderly and efficient transition from normal to emergency operations
- delegation of emergency authority
- assignment of emergency responsibilities
- authorisation by key personnel for actions contained within the plan
- coordination of efforts to cope with the emergency
- safe continuation of operations or return to normal operations as soon as possible.

Role of safety cases

In the same spirit as the SMS, safety cases should be used to provide structure to the various safety activities, to frame them under the same strategy and avoid loosely connected activities. In this sense, the safety cases should reflect the SMS strategy and structure.

Safety cases are used to demonstrate the safety of:

- an ongoing service
- a substantial change to that service.

Best practices agree that safety cases should not be produced for each change, but only when substantial changes are planned and if the resulting risks have a high severity (chosen severity thresholds are domain specific).

Human factors integration

The role of human factors in healthcare is of great importance. The delivery of care relies to a large extent on personal skills, professionalism and teamwork. The importance of human factors will increase as care pathways and systems become more complex and involve an increasing number of professions and disciplines working together seamlessly. It is, therefore, important that human factors are addressed systematically through a structured process that allows identification and management of issues related to human performance on an ongoing basis.

Human factors can be integrated into SMS activities if the analysis of human issues is structured in a disciplined process for (i) gathering information on the human component, (ii) identifying and prioritising relevant human factors issues, (iii) developing and implementing appropriate actions and (iv) monitoring the effectiveness of any actions taken.

Relevant human factors issues include:

- working environment
- organisation and staffing
- procedures, roles, responsibilities
- training
- teamwork and communication
- interaction with equipment.

Human factors approaches and data should be included for safety achievement (that is, reaching safety targets via SMS activities) and for safety assurance (that is, safety cases). In the latter case, a structured human factors process can be used as a form of backing evidence (process related, not direct) in safety cases.

Recommendations: Safety management systems

Five main recommendations can be made to healthcare professionals.

- Structure existing safety activities (and use of techniques) into a clear safety strategy and SMS. The best safety results are achieved by deploying a comprehensive and consistent safety strategy, not by the application of just one or more techniques. The SMS should collate all the existing activities, make interfaces and links between them clear, and highlight gaps or missing actions.
- Use safety cases to ensure systematic collection, integration and documentation of the evidence produced by all the SMS activities.
- Safety management is a process. Structuring an SMS ensures that a consistent strategy stays in place in the long term, but safety activities should provide a different focus and should be combined (or rotated) in the short to medium term. This ensures an effective use of resources and that no single safety activity drains all the resources.
- Integrate human factors considerations from the very beginning. The human contribution is crucial for healthcare so it cannot be left as a residual part, even though it may appear hard to manage.
- Use the SMS to clarify the internal and external interfaces – to ensure that safety people get the required input and provide the required output. This provides protection against undue interference and keeps the required communication channels open – for example, for staff feedback or input from the regulator.

In practical terms, the first things to be done are to (i) clearly define the safety policy, (ii) organise all the safety achievement activities, (iii) ensure the production of a clear documentation (safety case reports), and (iv) put in place safety assurance activities (the oversight function).

Chapter 6:

Key lessons – benefits, risks and issues for healthcare

From the existing experience of safety case practice in the reviewed domains, it is clear that the use of safety cases in healthcare carries both potential benefits and risks and challenges. These are explored below, followed by a discussion about issues deserving further investigation.

Potential benefits

Systematic, holistic thinking

Safety cases were explicitly introduced in a number of domains to encourage systematic and holistic thinking about safety issues. Prior to the introduction of safety cases, many domains relied upon prescriptive safety regimes whereby regulators (through safety standards) dictated the specific measures to be adopted to ensure system safety.

Safety cases provide a contrast to this approach. Firstly, this is through shifting responsibility for the justification and demonstration of safety clearly to the primary developers and operators of systems. Secondly, safety cases are often introduced hand-in-hand with a 'goal-setting' approach whereby high-level objectives are provided by regulators, but developers and operators are given freedom in establishing suitable arguments and evidence to demonstrate the achievement of those objectives.

Regulators will always struggle to be complete in prescribing regulations and requirements that are intended to apply to a large number and variety of applications. Regulators inevitably struggle in writing regulations that engage in the specifics of the day-to-day operation of every system to which the regulation applies. This is why the shift towards requiring developers and operators to demonstrate **their** systematic thought processes, and **their** systematic justification, is so important in striving for a comprehensive and holistic account of safety.

Integration of evidence sources

It is commonplace in existing practice that a diversity of evidence sources and types are required to demonstrate system safety – such as trials, human factors analysis, testing and operational experience. However, this diversity and amount of evidence can create difficulties. It can be difficult to judge completeness. Is the evidence set comprehensive? Does it cover all the issues? It can also be difficult to understand the distinct role and purpose served by each form of evidence. Safety cases help in this regard, by presenting the argument that explains how the overall safety objectives can be seen to be addressed through the assembled items of evidence.

Aiding communication among stakeholders

In existing safety case practice, at a minimum safety cases are developed by one organisation to be reviewed by another (a regulator). They enable the explicit documentation and communication of the beliefs and evidence as to why a system is acceptably safe. For most safety-critical and safety-related systems there are many stakeholders – for example, designers, operators, maintainers, managers, evidence providers and the public. Safety cases can act as a focus of discussion between these stakeholders. Each can provide input relating to

their understanding and concerns. Each can query the resulting safety case to see how their issues have been addressed.

Making the implicit, explicit

The act of establishing and documenting a safety case can help expose existing implicit assumptions and risk acceptance judgements. Having documented a case, it becomes easier to review the arguments, question the evidence and challenge the adequacy of the approach presented.

Aiding safety management and governance

Without an explicit safety case that attempts to pull together all the threads of the safety argument and ensure that appropriate evidence has been presented, there is a significantly greater risk of safety issues 'falling down the cracks' that can exist between existing safety assessments, metrics and arrangements representing the specific concerns of individual stakeholders or addressing single issues. Without the 'big picture' of a safety case, it is also easy for wildly varying and disproportionate amounts of effort to be spent on risk management. Alongside these safety risks, there is also the efficiency risk of duplication of effort in existing initiatives.

Potential risks and challenges

Becoming a paper exercise

Safety cases must not become just another 'filed return'. The production of a safety case is an opportunity for gaining greater understanding of the current picture of safety, and for potentially making safety improvements. However, to do this, it is important to ensure that appropriate time and effort is allowed for the development and review of safety cases. It is particularly important that a safety case review is thorough and systematic.

Being removed from everyday practice

Safety cases are supposed to address the realities of everyday system operation. It is important that they do not become a desk exercise that relates only dimly to actual practice. The primary concern of a safety case should lie in demonstrating safety, rather than being an exercise in attempting to shift liability or in merely demonstrating compliance with 'due practice'.

Being produced by the wrong people

It is important that safety case development involves all the relevant stakeholders with an understanding of, and involvement in, what actually makes systems safe (or unsafe). It cannot simply be produced by safety consultants or professional authors – even though they may be experienced in establishing apparently credible cases.

Issues requiring further consideration

The review of existing safety case practice, and the subsequent workshop, highlighted a number of issues that require further consideration as part of any move to adopt safety cases within the healthcare domain.

Understanding the motivation for the adoption of safety cases in healthcare

Safety cases have typically been introduced in domains where there has been a perceived weakness in the current safety assurance arrangements or where there have been significant safety problems (such as a major accident or – in the case of the FDA – a significant number of safety recalls). In order to provide a compelling case to those who may be involved in the production of a safety case, it is necessary to gain a clear understanding of where current practice falls short.

Identifying the owners of the safety case 'requirement'

In many of the existing domains, it can be seen that the development, review and acceptance of safety cases is **mandated** through regulators, regulations and standards. For example, safety cases are required as part of the licensing regime for petrochemical plants. While it is not unheard of for safety cases to have been developed by organisations without a regulatory requirement to do so, it is more common for them to become established practice through strong regulation and clear safety standards. It is, therefore, necessary to consider both the authorities and mechanisms (for example, standards, licences, contracts) that could potentially be involved in instituting a requirement for safety cases within the healthcare domain.

Identifying the 'target' for safety case development

As identified in the review of existing literature, most of the existing experience of safety cases in the healthcare domain has been from the development of safety cases for specific devices and IT systems. While this can be beneficial in its own right, it is necessary to consider whether there can be other (more overarching) targets for safety case development – for example, a care pathway, or the wider healthcare systems of a specific hospital or care home. It is worth considering where safety cases can make the biggest improvement in current practice. For example, if it is in the conjunction of people, procedures, protocols, devices and supporting IT systems that the biggest (and potentially unaddressed) safety issues are known to arise, then this would suggest that safety cases for overall healthcare systems should be a priority.

Identifying those responsible for safety case development

Identifying those potentially responsible for safety case development depends greatly on the 'target' of the safety case. In the case of the recent FDA regulation on medical devices (specifically, infusion pumps) the responsibility for safety case development was clearly assigned to the device manufacturers.

However, even in this relatively simple case, it could be argued that (analogous to the concepts of design safety case and 'user' or 'operational' safety case in the defence sector) there should be a corresponding operational safety case developed for the healthcare settings where these pumps are deployed. This would ensure that issues such as appropriate training, maintenance and limitations of use are addressed. For safety cases targeted at care pathways, some responsibility for safety case development may lie with the pathway 'designer', as well as those enacting the pathway in a particular healthcare setting.

Identifying the 'operational role' of safety cases

It is important to consider how a safety case regime could and would impact on everyday healthcare practice. If safety cases are developed without any expectation of them potentially prompting change and improvement in healthcare practice, the exercise becomes pointless and irrelevant. However, identifying particular mechanisms for the 'pull-through' of safety case observations and recommendations into day-to-day practice remains to be explored. It could be, for example, that the 'deep thinking' of safety cases could help establish and identify relatively simple interventions such as procedural checklists or local monitoring arrangements.

Identifying how a safety case regime could integrate with existing regulation

While the workshop conducted as part of this study helped to begin to identify the existing forms of regulation and oversight in the healthcare domain, further investigation is required into how safety cases could integrate with and support existing regulation. It is important that a clear and distinct role is defined for any safety case regime in order that it is not seen as valueless or a duplication of existing efforts.

Implementation considerations

The review of existing safety case experience, particularly of those domains where safety cases have been recently introduced (such as the automotive sector and medical devices in the US) has thrown up a number of practical implementation issues that need to be considered in any adoption roadmap.

- Consideration needs to be given as to whether there are (sufficient numbers of) suitably qualified and experienced personnel in place to help develop and review safety cases. While, as stated above, safety case development and review must directly involve those with first-hand experience in the domain, it will also be necessary to establish safety case facilitators who understand the processes of safety case construction and review.
- Significant effort would need to be made in the education and training of those involved in the safety case regime. Those responsible for development need to clearly understand the purpose of establishing safety case arguments and evidence. In addition to conveying the overall intent of a safety case regime, practical guidance will be required as to how to formulate

safety case arguments, select appropriate evidence and critically review safety cases. As part of this training, there is a need to develop safety case exemplars (perhaps of both good and bad safety cases), alongside review material for the community to access.

- The development of safety cases for applications already (perhaps implicitly) accepted as safe poses a potential risk of exposing weaknesses in existing arrangements. This is a good thing. However, contingency arrangements need to be in place to help address any problems exposed by the introduction of the new regime.
- Suitable arrangements would ideally need to be put in place for ongoing monitoring and review of the introduction of safety cases. Where safety incidents and accidents occur, they should be related back to the developed safety case to help identify necessary improvements to the specific safety case and safety case practice in general. It is also important to ensure that data are being collated in order to establish whether safety cases are (cost-effectively) improving the safety of day-to-day operations.

Specific recommendations

In order to move the findings of this research forward, two questions need to be addressed.

- Firstly, is there sufficient evidence of the value of safety cases in the healthcare domain?
- Secondly, even if the value of safety cases is established, could safety cases be introduced within the existing constraints of the healthcare domain?

Trials/pilot studies of the safety case approach

With regard to the first question, this study has been able to point to the experience of safety case practice in existing domains and outline an example of an operational safety case for a specific class of medical devices. However, further trials or pilot studies of a safety case approach within the healthcare domain are required in order to establish a credible evidence base for recommending a change of regulatory practice. Such studies cannot be done simply as a removed exercise by academics or safety consultants. They would need to involve the appropriate stakeholders – for both the development and review aspects of a safety case regime.

These studies need to experiment with the potential targets of safety case development. They need to explore the parameters of level, scale and resolution of the safety case. For example, while it may be interesting to conduct an 'in-depth' safety case development for a specific care pathway, the scalability and practicality of rolling out such a process across a large number of similar pathways would need to be considered.

It would also be very important, as part of any such study, to clearly establish the dimensions of safety case 'success' and establish suitable measures to be drawn from any experiment. In this report, we have already discussed the potential benefits in safety case regimes – for example, improved communication between stakeholders, improved safety and improved comprehension and understanding of safety concerns. Each of these aspects would need to be monitored in order to gain a good understanding of the 'case' for safety cases.

Further study on the implementation considerations

This study has highlighted a number of important (and, in many cases, practical) considerations that would need to be addressed in any implementation of safety case practice within the healthcare domain, such as its relationship to existing regulation and oversight arrangements. In addition to trials of the safety case approach, there should be a parallel study that explores each of these considerations with a view to establishing the feasibility of a safety case regime within the healthcare domain, and (if feasible) a suitable implementation roadmap. Should the results of the trials/pilot studies of the safety case approach be successful, the output of this feasibility study would provide the complementary information necessary to help roll out a safety case strategy for healthcare.

Summary box 4: Recommendations

Demonstration: clinical safety cases – Develop, and make available to the healthcare community, pilot studies and demonstrations of clinical safety cases in areas of recognised patient safety risk. These should be constructed bottom-up with the support of clinicians to ensure that they are clinically relevant and meaningful.

Evaluation: clinical engagement and measures of success – Define measures of success such as enhanced clinical engagement and improved communication, and investigate whether and through which mechanisms these are met by participation in the development of clinical safety cases.

Feasibility: regulation – Investigate with the regulator (the CQC), bodies with experience in the adoption of the safety case concept (such as Connecting for Health) and healthcare organisations whether the adoption of clinical safety cases is feasible as a regulatory instrument to contribute to a transparent regulatory process and to provide meaningful and relevant feedback on a clinical level to healthcare organisations.

Education: proactive patient safety management – Provide training and education to healthcare organisations, as well as NHS bodies and regulators, in systematic and proactive approaches to patient safety risk management through programmes such as Safer Clinical Systems.

Chapter 7:

Conclusion

This project reviewed current safety and regulatory practices in six safety-critical industries. A distinguishing feature of all the industries reviewed is the implementation of highly-structured approaches to safety management to ensure that organisations are proactively identifying, assessing, mitigating and monitoring risk. The safety case regime is a means of establishing a formal structure for these activities and ensuring that a disciplined and standardised approach to managing risk is adopted. In healthcare, safety cases could be a useful tool to promote structured thinking about risk among clinicians, foster multidisciplinary communication about safety and enhance clinical engagement in the regulatory process.

The UK is one of the leading countries in terms of technical expertise and practical experiences in the development and use of safety cases in safety-critical industries. There is an opportunity to provide thought leadership in patient safety through the transfer and appropriate adaptation of such practices in a healthcare context. Connecting for Health has already set an example with the production of guidance for the development of clinical safety cases as part of the National Programme for IT. In the USA, the Food and Drug Administration (FDA) is also promoting the adoption of safety cases for certain types of medical devices.

With all safety activities, the involvement and engagement of clinicians and frontline staff is an essential prerequisite, but often difficult to achieve in practice. For example, incident reporting – an important mechanism for organisational learning – has met with well-documented barriers to its successful adoption, such as a lack of transparency, lack of feedback and lack of ownership felt by frontline staff. We believe that the adoption of safety cases can foster multidisciplinary communication around patient safety issues and enhance clinical engagement. This claim needs to be validated through appropriate pilot and demonstration studies.

Safety cases are a way of providing structure to safety activities and integrating different types of evidence to provide safety assurance. However, this can only succeed when relevant stakeholders, such as clinicians, managers and regulators, possess a sufficient understanding of systematic and proactive approaches to safety management. With the Safer Clinical Systems programme, the Health Foundation is already leading the way in involving healthcare organisations in the development and adoption of structured, system-based patient safety approaches.

Collaboration and communication among the different stakeholders in patient safety is another important driver behind innovative approaches and solutions. The workshop held as part of this project brought together academics and experts in industrial safety with clinicians, patient safety managers and regulators. The dialogue that resulted brought new insights and helped to identify enablers and barriers to the useful adoption of safety cases in healthcare. This dialogue should continue in order to ensure that proposed solutions remain practicable and clinically relevant.

References

1 Ministry of Defence. Defence Standard 00-56: Safety Management Requirements for Defence Systems. *Defence Standard*; Issue 4: June 2007.

2 The Honourable Lord Cullen. *The Public Inquiry into the Piper Alpha Disaster*. London: HM Stationery Office; 1990.

3 Kelly T. *A Systematic Approach to Safety Case Management*. SAE International; 2003.

4 Maguire R. *Safety Cases and Safety Reports*. Ashgate; 2006.

5 EUROCONTROL. *Safety Case Development Manual (V2.1)*. 2006.

6 *The Offshore Installations (Safety Case) Regulations 2005 No.3117*. www.legislation.gov.uk/uksi/2005/3117/contents/made (accessed February 2011).

7 *The Control of Major Accident Hazards (Amendment) Regulations 2005 No.1088*. www.legislation.gov.uk/uksi/2005/1088/contents/made (accessed February 2011).

8 Health and Safety Executive. *Safety Assessment Principles for Nuclear Facilities*. HSE; 2006. www.hse.gov.uk/nuclear/SAPs/SAPs2006.pdf

9 *The Railways and Other Guided Transport Systems (Safety) Regulations 2006*. UK Statutory Instrument 2006 No.599.

10 EC Directive 91/440/EEC. *On the development of the community's railways*. 29 July 1991.

11 Health and Safety Executive. *COMAH Safety Report Assessment Manual (V2)*. HSE; 2006. www.hse.gov.uk/comah/sram/ (accessed February 2011).

12 Ministry of Defence. *Joint Service Publication JSP 430: MoD Ship Safety Management*. Ministry of Defence; Issue 1: January 1996.

13 International Organization for Standardization. *ISO 26262: Road Vehicles – Functional Safety*. BL 9 2007-07-20, 2007.

14 Haddon-Cave C. *The Nimrod Review: An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006*. The Stationery Office, ISBN 9780102962659.

15 Food and Drug Administration. *Guidance for Industry and FDA Staff – Total Product Life Cycle: Infusion Pump – Premarket Notification [510(K)] submissions*. www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm206153.htm#6

16 ISO 14971 *Application of Risk Management to Medical Devices*. 2007.

17 ISB 0160 *Health Informatics – Application of clinical risk management to the manufacture of health software*. DSCN 14/2009.

18 ISB 0129 *Health Informatics – Guidance on the management of clinical risk relating to the deployment and use of health software*. DSCN 18/2009.

19 Baker M and Harrison S. *Lessons from NHS Connecting for Health*. 2011. Presentation available at: www2.warwick.ac.uk/fac/med/staff/sujan/research/safety_case_review/wp3_workshop/baker_harrison_scr.pdf

20 IEC 80001-1 *Application of Risk Management for IT Networks Incorporating Medical Devices – Part 1: Roles, responsibilities and activities*. 2010.

21 Sujan MA, Harrison MD, Steven A, Pearson PH, Vernon SJ. Demonstration of safety in healthcare organisations. In Gorski J (ed) Computer Safety, Reliability, and Security. Safecomp 2006. *LNCS* 4166;219-232, Springer Verlag.

22 Programme and presentations available at: www2.warwick.ac.uk/fac/med/staff/sujan/research/safety_case_review/wp3_workshop/

Stay informed

The Health Foundation works to continuously improve the quality of healthcare in the UK. If you would like to stay up to date with our work and activities, please sign up for our email newsletter at:

www.health.org.uk/enewsletter

You can also follow us on Twitter at:

www.twitter.com/HealthFdn

The Health Foundation is an independent charity working to continuously improve the quality of healthcare in the UK.

We want the UK to have a healthcare system of the highest possible quality – safe, effective, person centred, timely, efficient and equitable.

We believe that in order to achieve this, health services need to continually improve the way they work. We are here to inspire and create the space for people to make lasting improvements to health services.

Working at every level of the system, we aim to develop the technical skills, leadership, capacity and knowledge, and build the will for change, to secure lasting improvements to healthcare.

The Health Foundation
90 Long Acre
London WC2E 9RA
T 020 7257 8000
F 020 7257 8001
E info@health.org.uk

Registered charity number: 286967
Registered company number: 1714937

For more information, visit:
www.health.org.uk

Follow us on Twitter:
www.twitter.com/HealthFdn

Sign up for our email newsletter:
www.health.org.uk/enewsletter

ISBN 978-1-906461-43-0