

# *forward*

*a future of reliable wireless ad hoc networks of roaming devices*

## An Investigation into System Security Requirements for Next Wave Information Provision Services - Part 1

March 23rd 2005

**Record of Changes**

Date	Version	Comment
23/3/2005	1.0	First Issue

**Authorisation**

Dr. Sadie Creese  
FORWARD Steering Committee Member

Date

## **Authors**

Andy Cole, QinetiQ, [ajcole@qinetiq.com](mailto:ajcole@qinetiq.com)

Sadie Creese, QinetiQ, [screese@qinetiq.com](mailto:screese@qinetiq.com)

Helen Roscoe, QinetiQ, [h.roscoe@eris.qinetiq.com](mailto:h.roscoe@eris.qinetiq.com)

Richard Winsborrow, QinetiQ, [rpwinsborrow@qinetiq.com](mailto:rpwinsborrow@qinetiq.com)

## Executive summary

This report on *An Investigation into System Security Requirements for Next Wave Information Provision Services- Part 1* forms deliverable D22 of the FORWARD<sup>1</sup> project.

Crucial to the successful exploitation of future pervasive computing technologies will be their ability to protect our safety and security. The aim of project FORWARD is to enable the development of trustworthy and flexible pervasive computing environments through the systematic investigation of some core issues, namely security, interoperability and quality of service. Underpinning the successful delivery of any technology, is an understanding of the requirements likely to be made of it; otherwise how can we measure success?

We report here the results of our research into the development of a methodology for capturing information security requirements. The methodology is designed to:

- Support the decomposition of system security requirements to a component level, which supports solutioneering and procurement from third parties.
- Provide a notation which directly links the assessment of assets requiring protection, the risk to those assets and the resulting information security requirements of the system. Further, the security requirements are directly linked to the system components delivering the solution, and the assurance requirements made of components of the solution so demonstrating how the assurance requirements support the overall security solution.
- Provide a graphical presentation of the system security argument which is intuitive to use and easily scalable.
- Provide a method for efficiently assessing the impact of environmental change on the requirements, solutions and assurance methods for the entire system.

The project has chosen to consider three scenarios, which together are designed to provide a mechanism for investigating a broad range of requirements applicable to many other applications.

- Scenario 1: Commercial Media Provision
- Scenario 2: Personal Digital Environments
- Scenario 3: Remote Monitoring of Health in the Home

We demonstrate the methodology via partial application to the three information provision scenarios. The scenarios are not complete, and the methodology has only been taken to the level before a technology or solution was selected. This is because we only intend here to demonstrate how to elucidate the security requirements of the case studies, and are not suggesting solutions or implementations.

The next stage in our work will be to conduct a more detailed requirements gathering exercise for one of the scenarios, so facilitating a capability gap assessment to be conducted. The overall results of this gap analysis will be a clear understanding of the security requirements for which no current solutions are adequate, and which will be crucial to future pervasive information provision services. This will be reported on in a separate document.

---

<sup>1</sup> [www.forward-project.org.uk](http://www.forward-project.org.uk)

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Purpose . . . . .	1
1.2	Strategy . . . . .	1
1.3	Background . . . . .	2
1.4	Structure of the Document . . . . .	3
<b>2</b>	<b>Developing System Security Requirements</b>	<b>4</b>
2.1	Approach . . . . .	4
2.2	Developing the system security requirements . . . . .	5
2.3	Developing Evidence Requirements . . . . .	8
2.4	Handling Safety and Security Critical Systems . . . . .	9
<b>3</b>	<b>Commercial Media Provision Scenario</b>	<b>10</b>
3.1	Scenario Overview . . . . .	10
3.2	Business Security Requirements . . . . .	11
3.3	Generating Evidence / Assurance Requirements . . . . .	18
<b>4</b>	<b>Personal Digital Environments Scenario</b>	<b>20</b>
4.1	Scenario Overview . . . . .	20
4.2	Business Security Requirements . . . . .	20
4.3	Generating Evidence / Assurance Requirements . . . . .	24
<b>5</b>	<b>Remote Monitoring of Health in the Home Scenario</b>	<b>26</b>
5.1	Scenario overview . . . . .	26
5.2	Business Security and Safety Requirements . . . . .	27
5.3	Generating Evidence / Assurance Requirements . . . . .	33
<b>6</b>	<b>Dynamic Risk Management</b>	<b>36</b>
<b>7</b>	<b>Conclusions and Future Work</b>	<b>38</b>
7.1	Results . . . . .	38
7.2	Validation and gap analysis . . . . .	38
7.3	Potential for tool support . . . . .	38
	<b>References</b>	<b>39</b>
	<b>List of Abbreviations</b>	<b>41</b>

**This page is intentionally blank**

# 1 Introduction

## 1.1 Purpose

This report on *An Investigation into System Security Requirements for Next Wave Information Provision Services- Part 1* forms deliverable D22 of the FORWARD<sup>2</sup> project.

The pervasive computing paradigm foresees communicating and computational devices embedded throughout our environment. Such devices will be capable of forming dynamic networks from wired and wireless infrastructures, utilising both back-bone pre-existing infrastructures and peer-to-peer communications. Potentially multiple heterogeneous networks will co-exist at any one location, offering users the ability to traverse at will, accessing unprecedented amounts of data and information supported by new ubiquitous services *nu-services*. In order to leverage the potential offered by the pervasive paradigm, mechanisms will be required which protect users against information over-load, and provide intelligent, intuitive interfaces to optimise interaction and service delivery. The resulting ubiquity of information networks may appear to offer a true ambient intelligence; users may store personal data to enable the facilitation of bespoke information services over whichever networks they chose to traverse, perhaps depending on artificial intelligence or agent technologies. Undoubtedly, these technologies will pervade our personal spaces; either through our own exploitation of their capabilities, or by our friends and family. Ultimately, it may not be possible for us to choose not to exist in such a technology environment (or even to switch some technologies off).

Crucial to the successful exploitation of future pervasive computing technologies will be their ability to protect our safety and security. However the technologies, resulting systems and services are becoming increasingly complex, and may possess emergent properties not conceived of in their design; some of which may impact on the systems's integrity. This is further antagonised by the dynamism of such systems; even if it were possible to produce a high-integrity system with no undesirable emergent properties, the system is likely to change rapidly introducing additional behaviours which may not respect the required integrity properties.

The aim of project FORWARD is to enable the development of trustworthy and flexible *ambient intelligence* environments through the systematic investigation of core issues: security, interoperability and quality of service. Crucial to the successful delivery of any technologies is an understanding of the requirements likely to be made of them. This is particularly challenging in the case of security as it requires a full understanding of what assets we wish to protect, who from, and to what degree. It is unlikely that we can fully comprehend the totality of security requirements for future pervasive computing systems, as we can only make an educational guess at future threat environments, the types of services we might wish to exploit and the assets we will be required to store digitally in order to utilise such services. However, without even a partial understanding of security requirements for such technology environments we will find it difficult to plan and develop solutions for the future. The project has chosen to focus on a certain type of application, that of information provision based services. It is likely that such services will be at the centre of pervasive technologies exploitation and so securing them both crucial and challenging.

## 1.2 Strategy

Our objective is to understand the information security requirements for future pervasive computing information provision services. However, consideration of requirements at the level of generic information provision services will only result in a superficial high-level capturing of security requirements; which is likely not to challenge current solutions, as requirements at this level are likely to be equally generic. Therefore, the project has chosen to consider three scenarios, which together are designed to provide a mechanism for investigating a broad range of requirements applicable to many other applications.

---

<sup>2</sup> [www.forward-project.org.uk](http://www.forward-project.org.uk)

- Scenario 1: Commercial Media Provision
- Scenario 2: Personal Digital Environments
- Scenario 3: Remote Monitoring of Health in the Home

Our strategy being to consider each scenario in turn, establishing the information security requirements in order to facilitate the capability gaps existing in current solutions to be identified.

Unfortunately there is no current best-practice methodology for developing system information security requirements which supports decomposition to a level appropriate for solutioneering. There exists a set of industrially developed risk assessment methodologies; these are an essential component of understanding the assets we need to secure and the risk to them. But the process of turning such high-level requirements into requirements against which solutions may be designed or procured remains the domain of information security professionals; informal methodologies and processes exist in the public domain but are not standardised upon. This lack of methodology will ultimately make it difficult to rigorously enforce security throughout a system's life-cycle; once a solution is in place it may quickly require review in the potentially fast-changing pervasive computing environment, as some solutions may no longer be appropriate or sufficient. What is required is a methodology which enables system level security assurance, for systems which are constantly evolving and which may be constituted from a combination of third party trusted and untrusted components. The methodology must support the decomposition of security requirements into parts suitable for solutioneering, in a manner which facilitates easy evolution of assurance arguments as risks and mitigation strategies necessarily change.

We report here the results of our research into the development of a methodology for capturing information security and assurance requirements. The methodology is designed to:

- Support the decomposition of system security requirements to a component level, which supports solutioneering and procurement from third parties.
- Provide a notation which directly links the assessment of assets requiring protection, the risk to those assets and the resulting information security requirements of the system. Further, the security requirements are directly linked to the system components delivering the solution, and the assurance requirements made of components of the solution so demonstrating how the assurance requirements support the overall security solution.
- Provide a graphical presentation of the system security argument which is intuitive to use and easily scalable.
- Provide a method for efficiently assessing the impact of environmental change on the requirements, solutions and assurance methods for the entire system.

We demonstrate the methodology via partial application to the three information provision scenarios. The next stage in our work will be to conduct a more detailed requirements gathering exercise for one of the scenarios, so facilitating a capability gap assessment to be conducted. The overall results of this gap analysis will be a clear understanding of the security requirements for which no current solutions are adequate, and which will be crucial to future pervasive information provision services. This will be reported on in a separate document.

### **1.3 Background**

The FORWARD project is part of the DTI sponsored Next Wave Technologies and Markets programme<sup>3</sup>. The aim of the programme is to ensure that UK business is structured and equipped to exploit the new information and communications technologies offered by the pervasive computing

---

<sup>3</sup> [www.nextwave.org.uk](http://www.nextwave.org.uk)

paradigm. In addition, the programme aims to foster viable markets with confident consumers so that U.K. citizens can enjoy the benefits offered by such future technology environments. The programme achieves this by supporting seven themed virtual interdisciplinary research centres (vIRC), integrating and disseminating the research via a knowledge transfer club. The FORWARD project is part of the *City and Buildings Virtual Research Centre*, whose focus is challenges in mobile appliance design, infrastructure integration, delivery architectures and interaction design.

#### **1.4 Structure of the Document**

This report is structured as follows. We begin in Section 2 by presenting our strategy for using Goal Structured Notation (GSN) in the development of system security requirements. We also discuss how our approach can be extended to cope with systems possessing safety requirements. Then in Sections 3, 4 and 5 we discuss the application of the approach to three case studies. In Section 6 we discuss how the approach can be used to document a specific security policy and architecture, facilitating dynamic risk management. Finally, in Section 7 we document our conclusions and focus for future work.

## 2 Developing System Security Requirements

### 2.1 Approach

We propose a methodology based on the use of current risk analysis techniques and the Goal Structured Notation (GSN). GSN [5], is a graphical notation currently used for documenting safety cases for critical systems. GSN has been developed over the last 10 years by the University of York, QinetiQ, and various other industrial partners as a means of capturing and presenting safety arguments. It is widely used in the safety community, particularly in military aerospace industries, where it is the de-facto standard for the presentation of safety cases. More recently we have been demonstrating how to utilise GSN in documenting security cases; in FORWARD deliverable D4, [4] it was used to demonstrate the security strategy for securing Bluetooth, as proposed by the Bluetooth Security Special Interest Group.

GSN is a notation for presenting logical arguments. It provides facilities for representing various types of information, such as context to the argument, assumptions and hypotheses. This makes GSN appropriate for representing most kinds of logical argument; a case for the security or safety of a system or component, or a justification for a policy or even a career strategy. GSN is particularly appropriate for use in capturing security requirements of a system or component since it enables the user to detail security requirements independently of solution type (technical or procedural) and specific implementations. It also provides a suitable mechanism for developing assurance requirements for the overall system, and the components of the system. Because the notation can be used to give clear requirements to solution components it could form the basis of contractual negotiations and the setting of acceptance criteria for third party systems and components. The notation also enables the user to directly relate specific security solutions and risk mitigation strategies to the security requirements they relate to. This facilitates dynamic risk management throughout the life of the system, as changes in threat can easily be assessed for their impact on security requirements and solution components. Should there be an impact it is easy to scope the degree to which the whole security strategy and architecture requires re-assessing, and which assurance evidence may be faulty. GSN can support the reuse of arguments through the use of templates, strategies and the reuse of components. This means that where a security case exists for the use of a particular component or class of system, it may be reused when developing the case for subsequent system evolutions, or even exported to an entirely separate system security case subject to the case delivering against the other systems security requirements.

For any given system or conceptual system model, the methodology for generating security requirements involves the following steps:

1. Identify business goals and assets to be protected.
2. Identify information security risk to those assets.
3. Utilising GSN, decompose security requirements until component solutions may be identified, including documentation of arguments given to justify decomposition.
4. Set requirements on integrity levels of any evidence demonstrating delivery against security requirements.

The resulting GSN diagram will then capture the system security requirements at a level appropriate for solutioneering, document the justification for such requirements and set requirements on any assurance evidence for solution components. The methodology is presented in Figure 1. Step 1 and Step 2 are actually outputs from any standard information security risk assessment, and we do not propose to investigate them further here<sup>4</sup>. Below we present more detailed explanations of Step 3 and Step 4, Step 5 is described in Section 6.

---

<sup>4</sup>We recommended that users of this methodology utilise a risk assessment in order to gather this information.

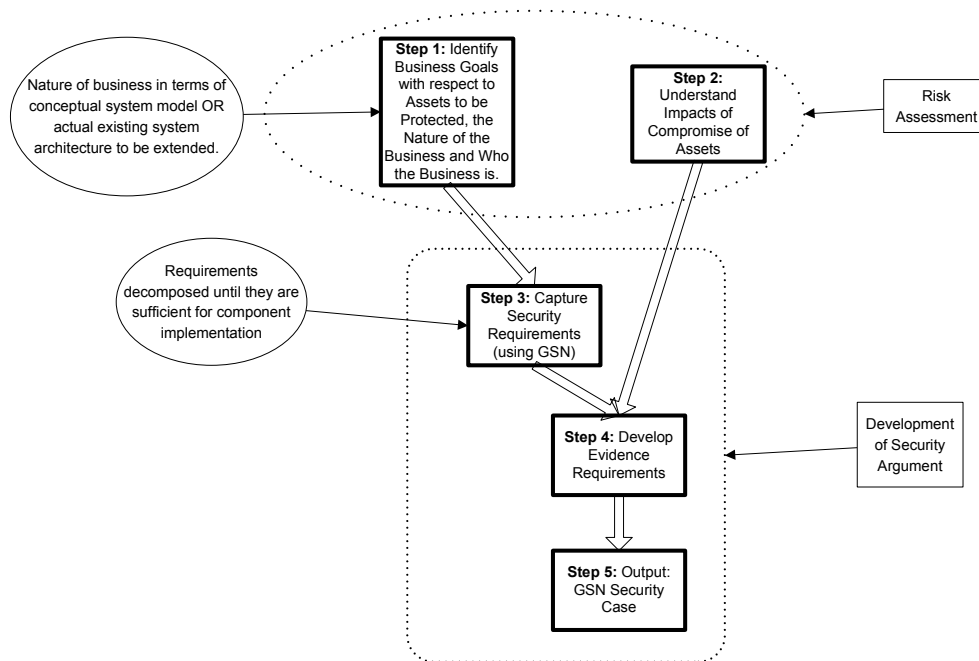


Figure 1: How the GSN and the Risk Assessments help create a Security Argument

## 2.2 Developing the system security requirements

### 2.2.1 High-level requirements and business context

Figure 2 below is a template for the high-level security requirements for each of the scenarios considered so far in FORWARD. Security requirements are strongly linked to business requirements. Businesses have to satisfy both commercial and legal requirements. These requirements include:

- Legal: Compliance with UK law, statutes and EU directives.
- Financial: Achieving return on investment, Earning income.
- Commercial: Protecting company name, reputation and assets, protecting and developing relationships with customers and suppliers.

Meeting these requirements are business goals. When considering a new product or service these goals will also have to be met in addition to the functional requirements. The business goals form the context for the design process. By considering these goals in the design and development process they can help to derive non-functional requirements for the product such as reliability, accessibility, confidentiality and integrity. By considering non-functional requirements in the context of business requirements it is possible to consider the cost of not meeting these requirements against the costs mitigating the risk. This enables possibly conflicting requirements to be resolved. Some requirements may be mutually incompatible. For instance the cost of achieving a level of security that adequately protects the company reputation and assets may make a new product commercially un-viable.

Assuming that Step 1 and Step 2 are complete we should have already identified the system security requirements at the highest level; what assets require protecting and how they are intended to be utilised by the system under consideration. In order to understand how to decompose such requirements we will need to understand the context of the highest level requirements; for example, the requirements will always have to be met in a financial and commercial context. This context will drive the lower level requirements and constrain the solutions. There will always be legal and commercial requirements. The legal requirements will depend on the application, and could include

the Data Protection Act, Privacy and Electronic Communications Regulations and other UK Law and EU Directives. The commercial requirements are to protect company assets such as name, reputation, intellectual property (IP) and relations with customers and suppliers.

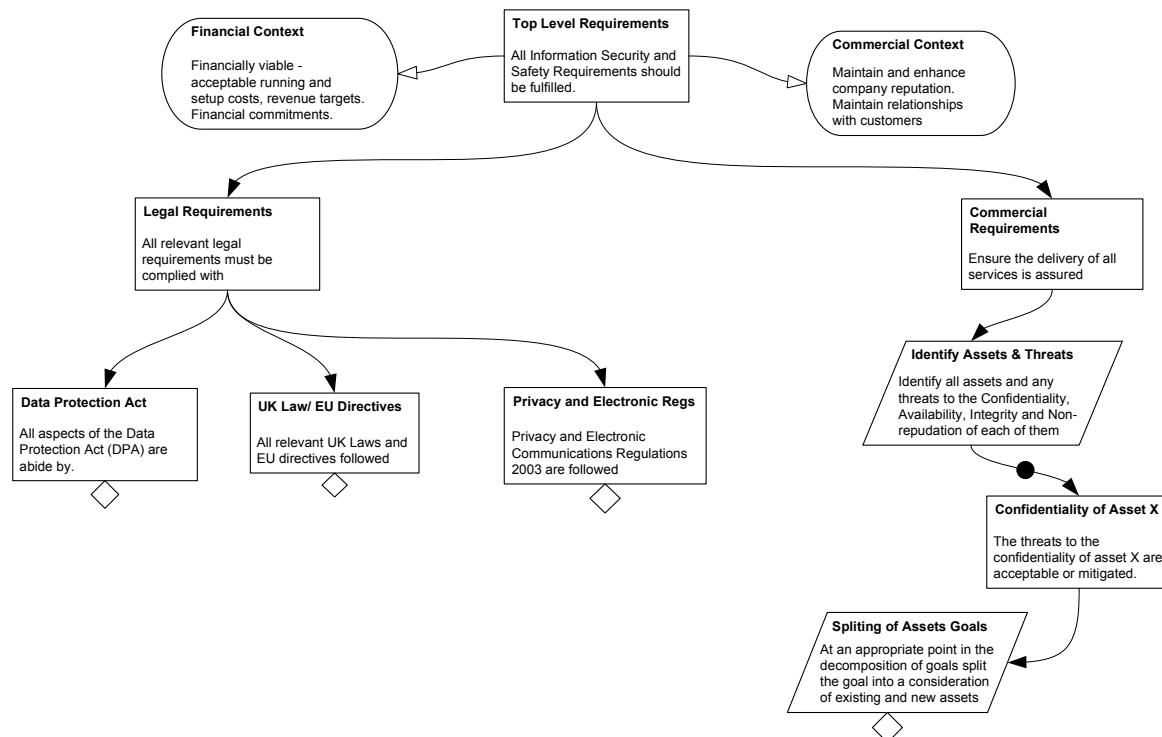


Figure 2: Template of the high-level security requirements

The reading of a GSN diagram is as follows:

- Rectangles represent *goals* or claims that some objective has been/can be achieved. In the tree structure, a goal is said to have been achieved if all its sub-goals have been achieved i.e. satisfaction of a goal depends solely upon the satisfaction of its explicit sub-goals. A goal can also be claimed to have been satisfied by direct appeal to some evidence a Solution.
- Circles represent *solutions*. These are direct evidence such as a reference to test results that demonstrates that some goal has been achieved.
- Rounded boxes are *context*, additional information to enhance understanding of the argument. They may for example provide definitions of terms or criteria for abstract requirement such as *adequately secure*.
- Contexts are usually attached to goals and are assumed to be applicable to all subsequent sub-goals in the hierarchy.
- Trapeziums are *strategies*, essentially comments explaining why a collection of sub-goals is expected to justify their parent goal.

A goal may be decorated with either a solid triangle or an open diamond. The latter represents an *unresolved goal*; that is, the argument is not complete. Providing a solution or sub-goals to address this goal is required to complete it. The former indicates that the goal decomposes further into another sub-tree. Arrows may be decorated by dots to indicate there are multiple sub-goals.

Through our examination of the the three scenarios, we found that the top-level requirements were very similar in all three situations. During this realisation we were able to create and evolve the template. The template is a top-level skeleton of the requirements and contexts that we believe

should appear in most situations when coming up with dependability requirements of a system. Additional goals and contexts can be added to the skeleton as the situation requires. For example, in the third scenario we found that an additional context to represent the clinical focus of the scenario was required.

The template consists of an uppermost top-level requirement to ensure the fulfillment of the information security and safety related requirements.

- **Top Level Requirements** - All information Security Requirements are fulfilled

The actual requirements a company is concerned about will be affected by a number of different factors, represented as contexts. We have identified two such factors that we believe will affect most situations, namely commercial and financial contexts.

- **Financial Context** - Relates to factors such as company targets and financial commitments.
- **Commercial Context** - Relates to the company's objectives such as maintaining company reputation and enhancing customer relationships.

The template shows the top-level requirement decomposed into two sub-goals: a legal requirement and a commercial requirement.

- **Legal Requirements** - All relevant legislation must be complied with.
- **Commercial Requirements** - Ensure the delivery of all services according to the business requirements, as detailed in the commercial context.

### 2.2.2 Legal Requirements

In most, if not all, situations a company will need to consider whether there are any laws or regulations that apply and show how they have been complied with. Thus the legal requirement splits into specific acts and regulations that may apply. In the template we have identified the Data Protection Act (DPA) and Electronic Regulations as possible laws and regulations that may apply, but there other UK laws and EU Directives that may be applicable.

- **Data Protection Act** - All aspects of the Data Protection Act must be complied with.
- **Privacy and Electronic Regulations** - Privacy and Electronic Communications Regulations 2003 have been followed.
- **UK laws and EU Directives** - Relevant aspects of UK Law and EU regulations are followed.

If a certain act applies in a particular situation then it should appear under the legal requirement goal, with a requirement that all relevant parts are complied with.

### 2.2.3 Commercial Requirements

The commercial requirements relate to assuring the delivery of the products or services provided by the company. To achieve this it is useful to identify all the different assets of the company, such as revenue and Intellectual Property (IP), and then consider the threats to Confidentiality, Integrity and Availability (CIA) and non-repudiation for each of them. This action of identifying assets and their threats is represented in the template as a strategy:

- **Identify Assets and Threats** - Identify all assets and any threats to the Confidentiality, Integrity, Availability and Non-repudiation of each of them.

Resulting from this strategy are multiple goals, indicated by the dotted arrow, one for each threat to an asset. For each threat there is a requirement that the threat is acceptable or somehow mitigated. For example, for a particular asset X there may be a goal for Confidentiality, one for Integrity, another for Availability and another for Non-repudiation, depending on the asset. Thus numerous sub-goals may result, for example:

- **Confidentiality of Asset X** - The threats to the confidentiality of asset X are acceptable or mitigated.

If the requirements are being generated for a system evolution the decomposition of each of the asset requirements must include both existing and new assets.

- **Splitting of Asset Goals** - At an appropriate point in the decomposition of a goal, split the goal into a consideration of new and existing assets.

This strategy may not immediately follow the initial asset goal, as the asset may need decomposing into different classifications of the asset before the existing and new separation can be done.

#### **2.2.4 Decomposition**

The requirements are then decomposed with respect to each asset and each security property of interest; authorisation, confidentiality, availability, integrity. Other factors, such as specific threats identified in the system risk analysis, could be considered to derive further requirements, and the process is then repeated until the required level of detail is achieved. Completion of the process results in an identification of security requirements at a low enough level so as to give clear criteria for solution components, and to link all security requirements clearly to the business context. The process is not complete if there are specific threats identified in the risk analysis for which no specific mitigation requirement exists. This completes Step 3.

### **2.3 Developing Evidence Requirements**

The level of evidence required for any particular component is determined by the impact and likelihood of the threat to the asset. The higher the risk then the higher level of evidence required. The types of evidence include conformance with development standards (rigorous or otherwise), and the application of design, protection, analysis and testing techniques. However, a components track-record may also be considered valid evidence. The higher the required integrity the more rigorous the methods used. The aim is to demonstrate, using a clear logical argument, that the system security requirements are met. It may be that some of the axioms are actually incorrect; for example, the argument may depend upon a certain piece of software behaving correctly, the evidence used to argue that the software met this requirement was based upon accreditation of the software, however, the accreditation of the component did not actually mean it was bug free and so that axiom of the argument was in fact false. The evidence should be sufficient to show that the risk is totally mitigated by the solution, or that the solution is able to sufficiently reduce the risk to an acceptable level. The type of evidence required for each particular component is documented as a strategy linking the actual component and the evidence within the GSN diagram.

Once the evidence requirements are set this completes Step 4. The result should be a clear understanding of security requirements at a level which solutioneering can be easily achieved. In addition, the assurance requirements for each component will also be identified; these will be optimal with respects to the role the components take in mitigating system risk.

## 2.4 Handling Safety and Security Critical Systems

The addition of a safety dimension will add additional context to the overall requirements, which is likely to place constraints on requirements for solution components. It will also make a significant difference to the types of assurance evidence considered acceptable.

Security and safety are used to categorise events on the outcome and the source of the risk. In commercial applications security is associated with malicious or criminal acts, typically cyber attacks, where the damage is financial or an infringement of personal rights such as privacy. Safety describes outcomes where human life, health and, increasingly, the environment are damaged. It may not be helpful to think of safety and security in isolation of each other or in different ways. The separation between safety and security is not always clear. For instance for some systems malicious acts and system failures could result in both financial and human harm. The need to make a product secure or safe comes from the application and the affect of the failure of that application. For instance if the result is financial this generates a security requirement and if it results in a loss of human life then there is a safety requirement.

An important part of handling systems with both safety and security requirements is understanding what are appropriate evidence levels. In the security domain Common Criteria uses Evaluation Assurance Levels (EALs), and in the safety domain Safety Integrity Levels (SILs) are used to infer the integrity of components. The EAL and SIL approach could be adapted as a measure of the level of evidence. EALs and SILs both categorise evidence levels, 1-7 for EALs and 1-4 for SILs. This could be adapted where there are recommendations for minimum acceptable evidence for each level. One limitation of Common Criteria is the cost of supplying the generic evidence for a component. The evidence could be tailored to meet specific requirements. For instance integrity and availability may be important, but confidentiality may not.

To illustrate the use of GSN and the scope of re-use we have developed GSN arguments for each of the scenarios, these are described in the next three sections.

### 3 Commercial Media Provision Scenario

The aim of Scenario 1 is to explore the security implications of using pervasive computing technologies to provide new ways of delivering information services to the citizen 'on the move'. The scenario focuses upon an art exhibition context, in which the exhibits are installations that exploit information and communication technologies in innovative ways to create multi-media experiences. By using location-based services delivering installation-specific information and stimuli to an individual's personal communications device her or his appreciation (and perhaps experience) of an installation can be augmented. The security implications could equally well apply to other applications which need to deliver information that is more or less correlated with the location of the recipient, and which need to be able to adapt to the capabilities (and constraints) of a range of portable reception devices.

The delivery of location-based, context aware information to mobile phone users is already a practical proposition. Several wireless network technologies, in particular 802.11(WiFi), can support location identification. Mobile phone technologies allow a location accuracy of the order of 100 metres (when making use of triangulation and timing measurements). By way of contrast WiFi technologies offer the prospect of a location accuracy of the order of 1 metre (based on signal strength measurements). This suggests that these latter technologies could be used to track people (or things) in relatively confined locations with a degree of accuracy that establishes their position in relation to fixed objects of the size of furniture, equipment and vehicles.

The evolution and increased market penetration of these technologies (e.g. 3G mobile, variants of 802.11) is also leading to the development and use of more advanced portable devices with significant computing and media presentation capabilities. These exploit the regularly increasing capability of semiconductor devices to deliver cost-effective portable products for business, domestic, personal and entertainment uses. For instance, digital audio devices, mobile phones with colour displays and cordless headsets are becoming commonplace. Likewise digital radio and digital TV technologies are changing the context of communications for broadcast wireless communication. In fact, it is evident from a cursory look on the web that the integration of PDAs, mobile phones, MP3 players and their attendant multi-network capabilities (e.g. WiFi, 3G, Internet) in products is advancing apace.

#### 3.1 Scenario Overview

MediaSpace is an arts and sciences experience company whose high-level objective is to provide people with access to innovative and thought provoking installations. This is currently achieved via three spaces within the UK (London, Bristol and Lyme Regis). The galleries currently deliver the customer experience via physical installations, such as interactive sculpture, pictures and written text. In addition the company provides portable MP3 players to supply audio commentary in multiple languages. The company also use a web-site for providing limited information on each space.

MediaSpace wish to deliver their experience to as many fee-paying customers as is possible. Their development manager has identified pervasive computing technologies as potentially providing new interfaces and channels over which they might sell their services. However, the company currently has to spend large amounts of money securing their portable MP3 players against theft. Therefore, they wish to deliver their content direct to a customer's technologies. In addition to reducing costs associated with securing rented technology, this could also have the added benefit of providing experience to users across their preferred media rather than one dictated by MediaSpace.

The current pervasive technologies which MediaSpace would like to embrace are:

- Mobile Phones
- Portable MP3
- Portable DAB Radios
- Palm Held Computers

Any solution must facilitate easy evolution and delivery to new devices as they become available to the general public. In addition, the solution will be required to support electronic payment via the customer's choice of device. It is expected that the information interactions will be facilitated via a wireless connection, which will be chosen in response to the information security requirements.

### 3.2 Business Security Requirements

MediaSpace hope to improve the existing system for the delivery of audio commentary to their visitors using pervasive technologies. To be successful it is important to be able to understand the requirements of the system and assess the risks that the requirements are not met and from this establish the evidence required to show that the requirement will be met.

- **Top Level Goal** - All information Security and Safety Requirements are fulfilled

The top-level business requirement must be achieved in a financial context.

- **Financial Context** - MediaSpace must satisfy its own the financial requirements.
- **Commercial Context** - MediaSpace must satisfy its commercial requirements, such as maintaining the company reputation.

The cost of providing and maintaining the service must be acceptable. The financial requirements set the context for the technical requirements. The service has to financially viable; if the cost of the running the service is greater than the revenue that it generates then it cannot be justified. The cost of setting up and running the service is determined by the technology used. The costs will not be limited to the cost of buying equipment, but will also include the cost of making the system meet all the system requirements, such as the requirement for secure payment.

From a business management perspective MediaSpace is focused on assured delivery of its services, revenue assurance, compliance with laws, regulations and contractual requirements, protection of confidential and copyrighted materials and the protection of its reputation. Addressing this management agenda demands that MediaSpace identifies, amongst other matters, its requirements for securing its services and systems. Each of these concerns become a top-level requirement in meeting the requirements that adequate information security is provided. As documented in Figure 2.

These requirements can be decomposed into:

- **Legal Requirements** - All relevant legal requirements must be complied with.
- **Commercial Requirements** - Ensure the delivery of all services is assured.

#### 3.2.1 Legal Requirements

Over and above obligations to customers and suppliers there also are legal requirements. These legal requirements would have to be identified. In this example the Data Protection Act and the Privacy and Electronic Regulations have been identified. There are also other UK laws and EU Directives that may be applicable. The requirements of these laws have to be met.

- **Data Protection Act** - All aspects of the Data Protection Act must be complied with.
- **Privacy and Electronic Regulations** - Privacy and Electronic Communications Regulations 2003 have been followed
- **UK laws and EU Directives** - Relevant aspects of UK Law and EU regulations are followed.

### Data Protection Act

MediaSpace systems may store personal data. If this is the case then the storage of this data has to comply with Data Protection Act (DPA). This data may not be limited to personal data of the users of the Audio Commentary System. The threat of the system allowing unauthorised access to personal data stored on any other systems has to be considered.

- **DPA Aspect 1** - Personal Data is only kept so long as it is required
- **DPA Aspect 2** - People can access their stored Personal Data
- **DPA Aspect 3** - Unauthorised access to the stored Personal data is prevented

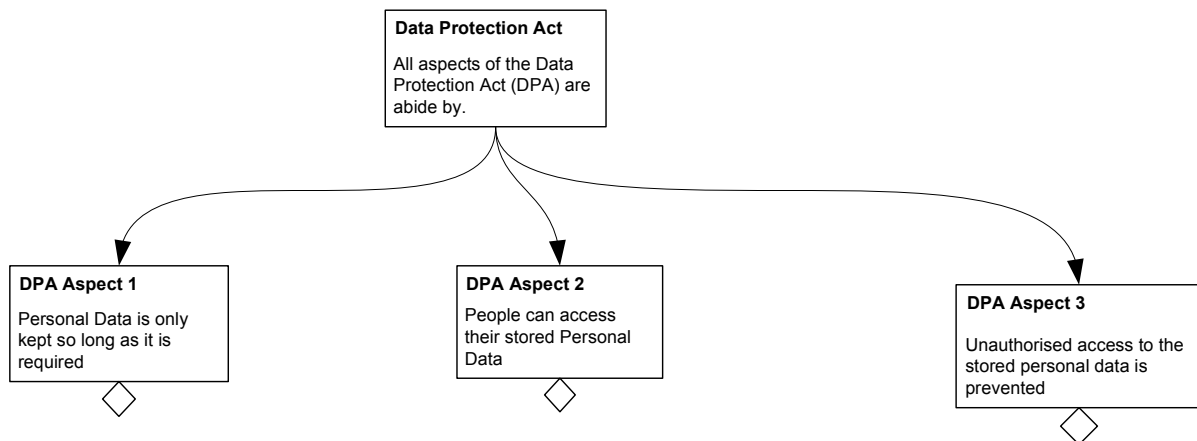


Figure 3: Data Protection Act

### 3.2.2 Commercial Requirements

MediaSpace's commercial requirements are derived by a strategy of identifying business assets and considering threats to those assets. Threats considered here are losses of Confidentiality, Integrity and Availability (CIA) and Non-Repudiation. The assets for MediaSpace are its services, its revenue and related Intellectual Property (IP).

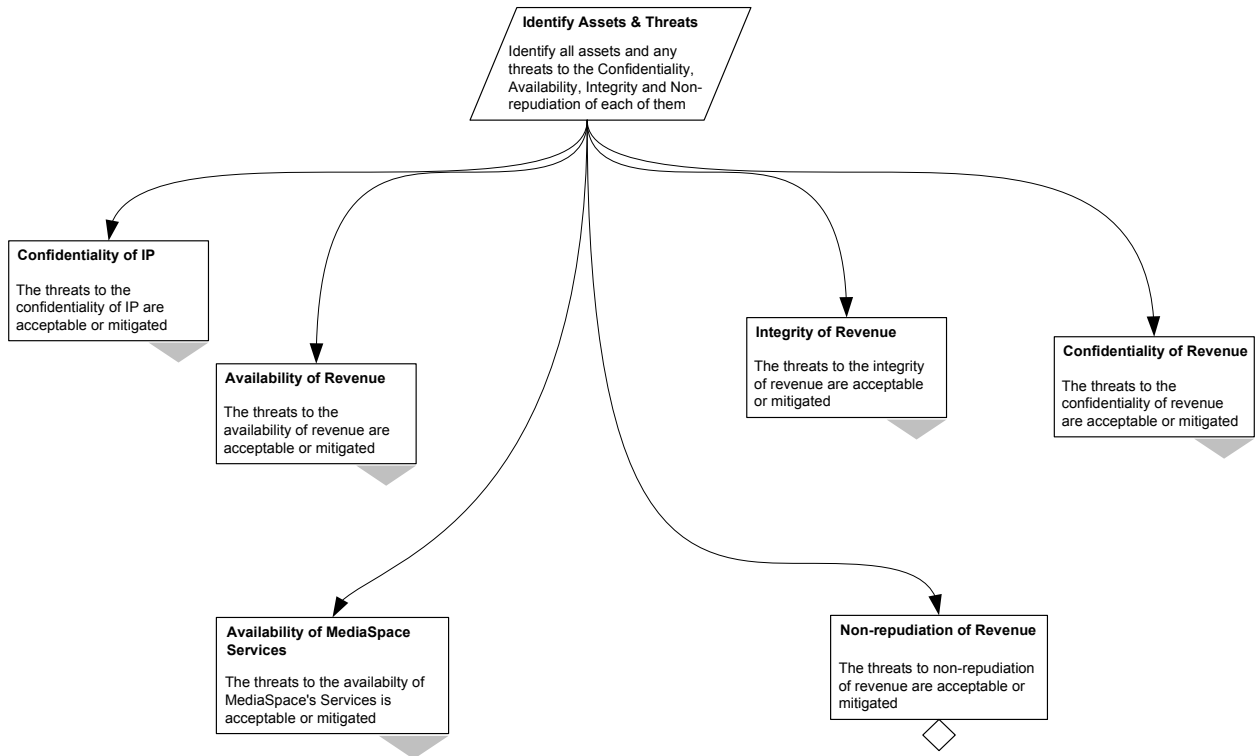


Figure 4: Scenario 1 - Assets and Threats

- **Availability of MediaSpace Services** - Ensure that MediaSpace services are available both to its visitors and to MediaSpace itself.
- **Confidentiality of IP** - Ensure the IP of the company and that of any related company is protected.
- **Availability of Revenue** - Ensure that revenue can be obtained from visitors.
- **Integrity of Revenue** - Ensure that the integrity of revenue is maintained. The amount received as a payment for the service must be correct.
- **Confidentiality of Revenue** - The details of the payments made by visitors should remain confidential .
- **Non-Repudiation of Revenue** - Ensure non-repudiation of revenue. It must be possible to show which payments have been made to ensure that services are not used without payment and that payment is correct.

#### Availability of MediaSpace Services:

Services will not only be provided to customers, they will also be used within MediaSpace. If the services fail they will disrupt the operation of MediaSpace and harm their commercial requirements.

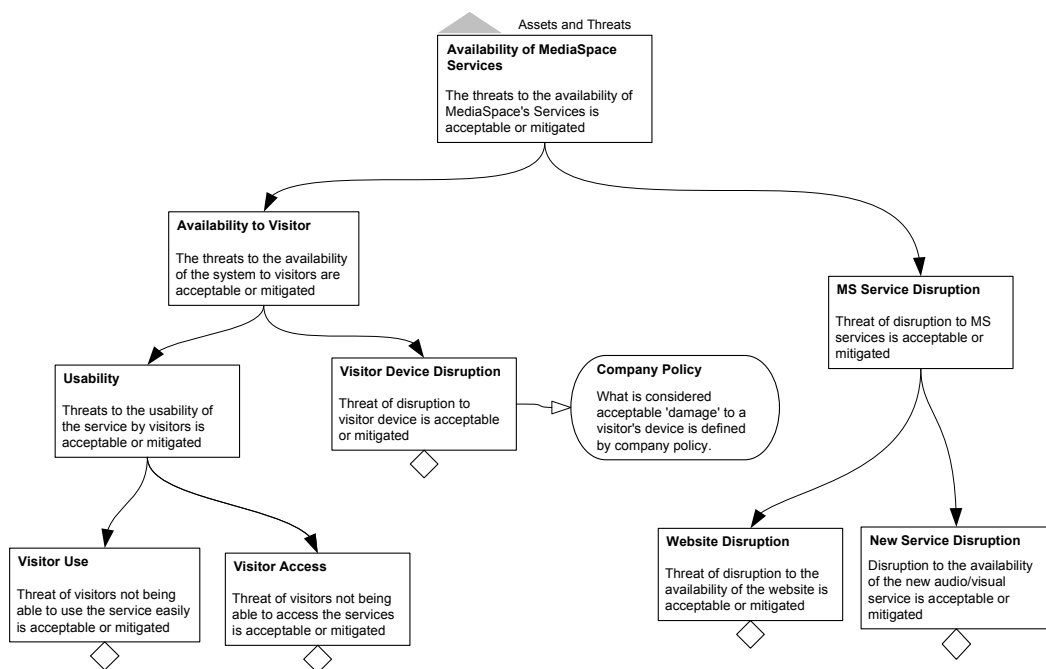


Figure 5: Scenario 1 - Availability of MediaSpace Services

- **Availability to Visitor** - Ensure that MediaSpace services are available to visitors.

MediaSpace want to provide services to its visitors on visitor owned equipment. The interface with this equipment must remain available and the visitor device must not be adversely affected.

- **Usability** - Visitors must be able to use MediaSpace's Services.

This creates two subgoals:

- \* **Visitor Use** - Visitors must find the service acceptably easy to use. This potentially conflicts with other goals as security measures may complicate the usage of the system.
- \* **Visitor Access** - The system must be accessible by equipment used by authorised visitors. This is a technological requirement that the devices chosen are available and reliable enough.

- **Visitor Device Disruption** - Visitor devices are not disrupted by connecting to the system. The MediaSpace visitors will be connecting their own equipment to MediaSpace equipment. MediaSpace's equipment must not damage a visitor's equipment or data stored on it.

This requirement is considered in the context of what MediaSpace considers damage to the visitors equipment to be:

**Company Policy** - This context describes the company's policy as to what constitutes damage to the visitor's device. This needs to be considered as the visitor's idea of damage may differ from the company's. For example, the visitor may consider the storage of cookies as damage, whilst the company may not.

- **MS Service Disruption** - MediaSpace's services are not disrupted.

The effects of disruption could be focused on the provision of the new service or on other MediaSpace services. For the purposes of this scenario, we have assumed that disruption to other MediaSpace services is limited to the company website. There may be other services that could also be adversely affected.

- **Website Disruption** - MediaSpace website is not disrupted.
- **New Service Disruption** - The availability of the new service must be acceptable.

### Confidentiality of IP:

MediaSpace owns its own IP and uses, under licence, IP from its suppliers. This IP needs to be protected against unauthorised use and copying. The IP may be contained in the audio commentary supplied to the MediaSpace customer or in other systems to which the new equipment could allow accidental or malicious access. The threat is to both stored IP and IP when it is being transmitted.

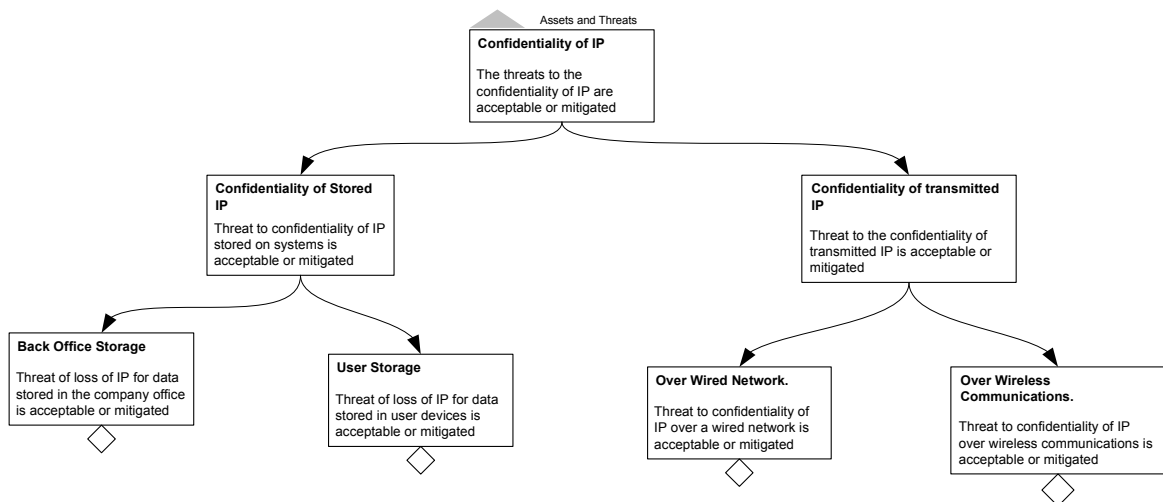


Figure 6: Scenario 1 - Confidentiality of IP

IP Protection can be split into the following sub-goals:

- **Confidentiality of Stored IP** - Unauthorised use of stored IP is prevented.

MediaSpace will store a complete set of audio commentary. The commentary system should not allow unauthorised access to other IP stored in other MediaSpace systems.

- **Back Office Storage** - Unauthorised use of other stored IP is prevented. MediaSpace store IP material belonging to both MediaSpace and third parties for use in its back office. Much more material could be stored and MediaSpace may not have permission to share all of the third party material, so the impact of not meeting this goal is high.
- **User Storage** - Unauthorised use of stored audio commentary IP is prevented. There is permission for authorised visitors to access the audio commentary so the impact is less.

- **Confidentiality of Transmitted IP** - Unauthorised use of transmitted IP is prevented.

The threats here are that there is unauthorised access to transmitted IP or that an authorised user misuses the IP. The impact is limited because the amount of IP is limited.

MediaSpace is allowing customers to load the commentary on to customer owned devices so it may be difficult to protect this IP from misuse. MediaSpace could choose to protect the IP by limiting the downloaded material to prevent it from being copied. This however could be technically difficult and expensive. So MediaSpace may have to choose to give this IP away. MediaSpace use wireless communications to communicate with visitor devices and a wired network to connect other systems and to connect to the internet, hence the two sub-goals are:

- **Over Wired Network** - Unauthorised access to the MediaSpace Network must be prevented. This potentially has a higher impact because this network gives greater access to MediaSpace systems and data.
- **Over Wireless Communications** - Unauthorised access to the MediaSpace wireless network must be prevented. Wireless communications should be limited to the data intentionally transmitted to visitors. So the impact of unauthorised access is limited.

**Availability of Revenue:**

Visitors should not be able to access MediaSpace services without full payment. This has a single sub-goal of Underpayment; a visitor gains access without paying fully for the service.

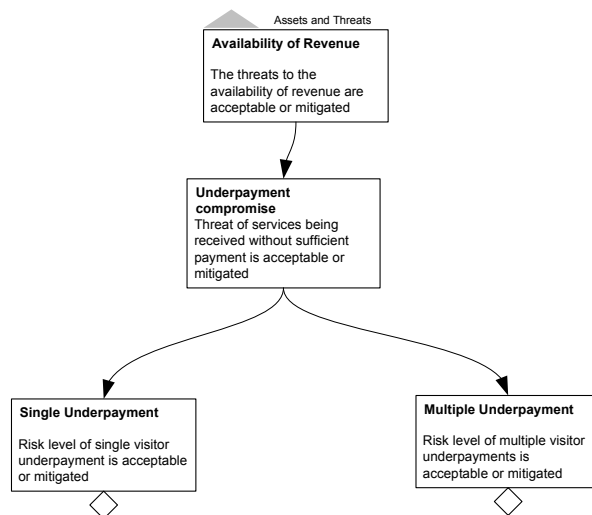


Figure 7: Scenario 1 - Availability of Revenue

- **Underpayment Compromise** - Visitor payments are not lost and visitors cannot gain access without full payment.

The impact of this will depend on whether it is a single or multiple events. The reason for considering them as separate cases is because the likelihood and impact of a successful exploit is different as are the likely control mechanisms.

- **Single Underpayment** - A single visitor gains access to the service without paying fully. The impact of this is low.
- **Multiple Underpayment** - Multiple visitors gain access to the service without paying fully. The impact of this is high.

**Integrity of Revenue:**

To demonstrate how the tree would expand further, we have extended the subtree for this requirement to include the strategy for determining the evidence requirements and the evidence goals to mitigate the identified risk. The evidence requirements depend on the solution or technology implemented.

There is a single sub-goal of the overpayment by a visitor:

- **Visitor Overpays** - Visitors are not overcharged. The strategy for the goal is to conduct a risk assessment. This identifies two cases.

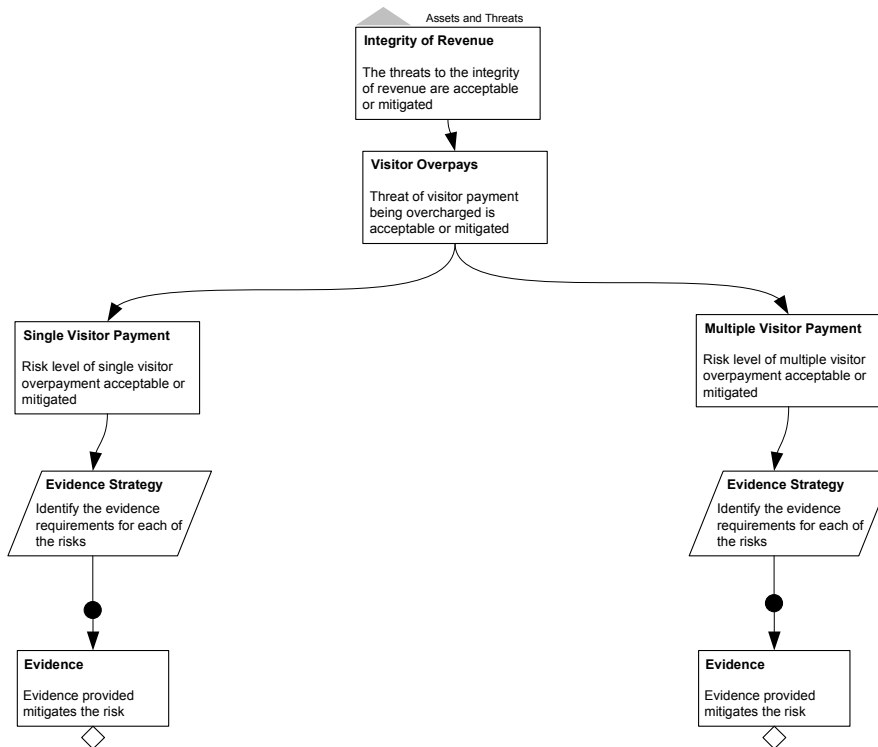


Figure 8: Scenario 1 - Integrity of Revenue

Whether the compromise is a single or multiple event will determine the impact on the business. Thus we consider these two cases separately:

- **Single Visitor Payment** - This only affects a single visitor so the impact is less than for multiple visitors. This goal would be satisfied by identifying evidence that the risk has been mitigated. The strength of the evidence required being determined by the level of risk.
- **Multiple Visitor Payment** - This has a higher impact because more customers will be affected and the cost of refunding the loss will be greater. This goal would be satisfied by identifying evidence that the risk has been mitigated. The strength of the evidence required being determined by the level of risk.

#### Confidentiality of Revenue:

To make a payment the visitor is giving their payment details; this information must remain confidential. Payment details could be used to divert payment away from MediaSpace or defraud the visitor in other ways.

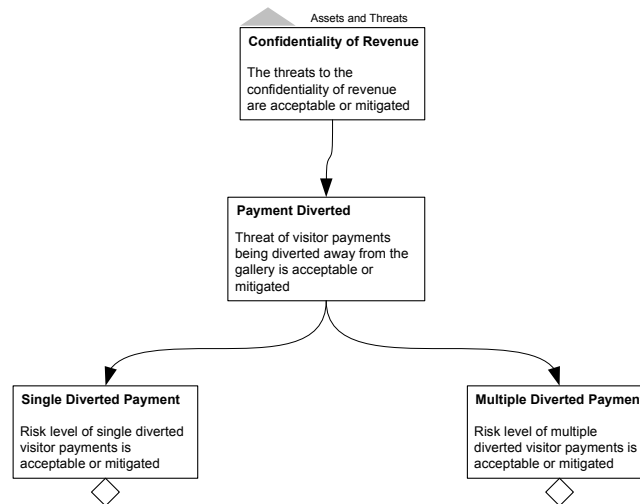


Figure 9: Scenario 1 - Confidentiality of Revenue

- **Payment Diverted** - Visitor payments are not diverted and are received by MediaSpace.

This compromise is again considered according to the number of events involved. Thus the impact of single and multiple events are addressed as two sub-goals:

- **Single Diverted Payment** - A single payment should not be diverted. As a single event the impact of failure is lower.
- **Multiple Diverted Payments** - Multiple payments should not be diverted. This includes payments from multiple visitors being diverted or more than a single payment being taken from a single visitor. The impact of this event is higher.

### 3.3 Generating Evidence / Assurance Requirements

The table below describes a range of incidents and a measurement of the risk associated with them (normally output from a standard risk assessment).

Incident	Impact	Likelihood	Measure of Risk
Visitor privacy compromise	L (localised)	L	L
	M (general)	L	M (-)
Visitor payment compromise	M (localised)	L	M (-)
	H (general)	L	M (+)
Visitor device disruption	L (localised)	L	L
	M (general)	L	M (-)
MediaSpace service disruption	H	H	H
IP protection	L (localised)	L (if DRM in operation)	L
	H (general)	H (if no DRM)	H

Key to Table:

L=Low; M=Medium; H=High; DRM=Digital Rights Management

The analysis presented in this table assumes that the MediaSpace systems are relatively well-protected and controlled whereas visitor equipment and the wireless network environment are not under a strong control regime.

One of the requirements identified earlier via Goal Structured Notation (GSN) was that the threat of visitors overpaying was acceptable or mitigated. Since this is classed as a compromise of visitor payments, examining the table reveals that this risk has a medium impact and risk, and a

low likelihood when the effect is localised to one visitor, but has a high impact and fairly high risk when the compromise is more global. This suggests that higher confidence requirements are needed to show that the global threat had been mitigated than the local threat.

The other risks can be linked back to the GSN requirements in a similar way, with the measure of risk indicating the level of evidence required to show that the risk has been mitigated.

## 4 Personal Digital Environments Scenario

The aim of Scenario 2 is to examine the security implications that might emerge for pervasive computing technologies that have yet to be developed. It involves the construction of a personal area network from a number of different types of wearable devices. The devices will be designed with the ability to communicate together intelligently via some form of wireless communications.

The Personal Digital Environments (PDEs) described in this scenario are characterised by their reliance on wireless network technologies and on the ability to dynamically meld ad hoc assemblies of devices into a PDE. Many of the barriers to interference with more traditional ICT systems with their (more or less) fixed configurations and strict change control philosophies are absent in this scenario.

Because the technology to implement a PDE does not currently exist, the requirements reflect what the PDE as a whole needs to be able to do rather than what requirements the individual devices need to have. When the PDE is refined and the implementation details decided, the PDE will most likely be made up of various different devices communicating on a wireless network, which together should fulfil the requirements identified. However, for now we shall identify the requirements associated with the PDE as a whole.

### 4.1 Scenario Overview

A technology R&D company are developing a technology designed to create an intelligent personal area network. The network will be constructed from wearable devices, communicating via some form of wireless communications. The purpose of the network is to deliver information procurement, delivery and management to the user. In addition the network must also provide the user with a mechanism for digital payment or a portable electronic purse. The Personal Environment will enable:

- The automatic gathering of information about the users declared interests, such as a favourite music group, gossip regarding a favourite celebrity or sports highlights and results.
- The automatic storing of such information such that the appropriate device can be easily used to access the information. E.g. music must be accessible to the best audio delivery device for the purpose, likewise for pictures and links to web-sites.
- The Environment must be easily configurable by the user to provide alert mechanisms, and to choose preferred delivery devices.
- The Environment must provide a secure payment mechanism with limited and intuitive interactions required by the user.
- All devices must be able to provide storage, and the Environment as a whole must provide dependable access to stored information.
- The Environment must support easy evolution to include new devices, both for temporary relationships involving transactions, and for the addition of new wearable devices requiring longer-term membership.

### 4.2 Business Security Requirements

In order to create a secure personal environment it is important to be able to understand the requirements of the PDE as a whole; the requirements of both the networking infrastructure of the PDE and the PDE devices that will communicate via the network. All the risks associated with a requirement not being met need to be assessed, and as a result the evidence to demonstrate that the requirement will be met identified.

As with Scenario 1, the top-level template applies (Figure 2), with the uppermost business requirement being that the system provides adequate information security and safety. In this scenario

the meaning of adequate is again influenced by financial and commercial factors, considered as the context within which the technology needs to be developed.

- **Top Level Goal** - All information security and safety requirements should be adequately fulfilled.
- **Top Level Contexts** - Financial Context, Commercial Context
- **Financial Context** - As with scenario 1, the R&D Company must satisfy its own financial requirements. In the development of the requirements of the technology, the company must bear in mind research, development, setup and running cost levels, revenue targets, and consider whether the technology is financially viable.
- **Commercial Context** - The commercial requirements of the company must also be taken into consideration, such as maintaining the company reputation.

Following the top-level template leads to the decomposition of the top-level goal into two sub-goals: legal requirements and commercial requirements, the commercial requirements being related to assured delivery of the product, and the legal requirements indicating laws and directives that need to be complied with.

- **Legal Requirements:** All relevant legal requirements must be complied with.
- **Commercial Requirements:** Ensure the delivery of the product/service is assured.

#### 4.2.1 Legal Requirements

Although not all of the laws, regulations and directives listed in the template may apply, they should always be considered, with requirements being generated if appropriate. Thus, the legal requirement branch, as shown in the template should always appear in the Goal Structured Notation (GSN) diagram, with the goals for those laws and regulations relevant to the scenario being expanded as needed.

#### 4.2.2 Commercial Requirements

When determining what the commercial requirements of the system are, it is useful to start by thinking about the different assets that need to be considered and what non-functional properties of them are required. Thus, a strategy to identify all assets and the threats to the Confidentiality, Integrity and Availability (CIA) and Non-repudiation for each of them.

- **Identify Assets and Threats Strategy** Identify all assets and identify the threats to the CIA and Non-repudiation for each of them.

For scenario 2, an asset is the data held within the PDEs, with consideration of the threats to the availability, integrity and confidentiality of the data as requirements. Likewise with the PDEs themselves, there are requirements that the threats to the integrity, confidentiality and availability of the PDE be acceptable or mitigated. We assume another of the assets to be revenue, although it is not clear how the company will generate it, with requirements to ensure that the threats to the confidentiality, availability and non-repudiation of the revenue are acceptable or mitigated.

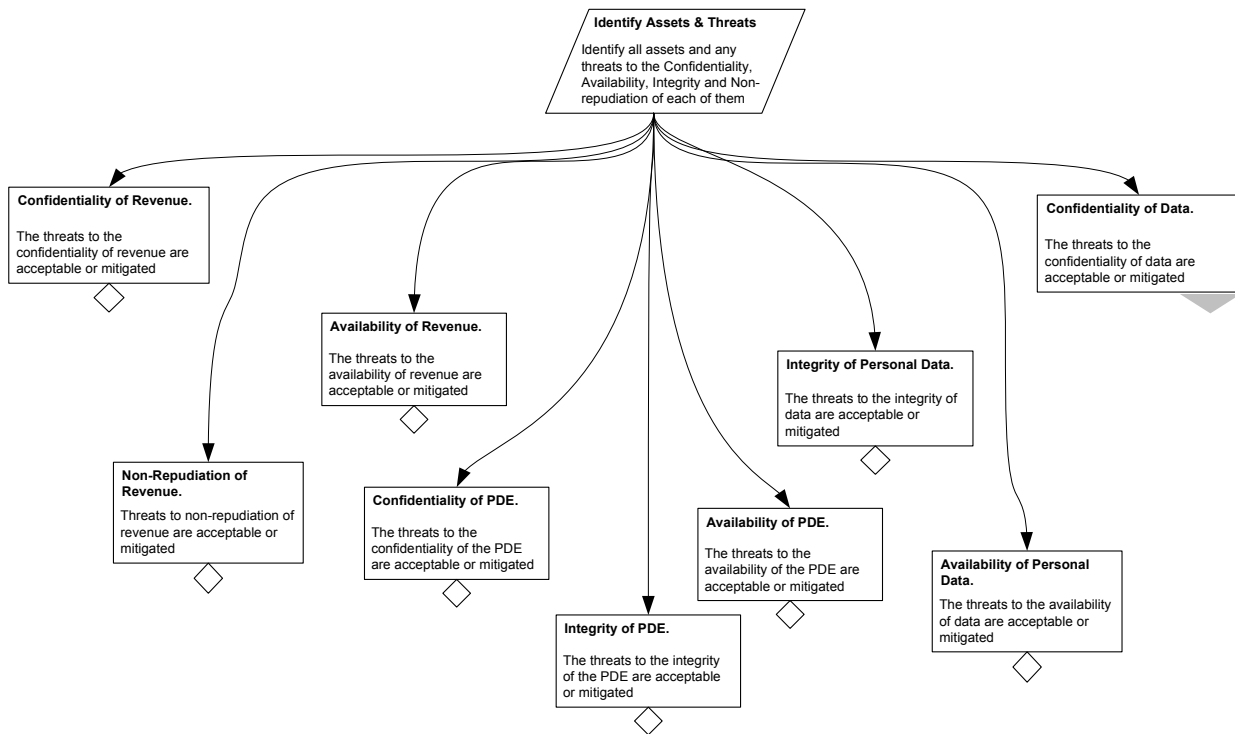


Figure 10: Scenario 2 - Assets and Threats

Thus, the commercial requirements can be decomposed into the following sub-requirements:

- **Integrity of PDEs** - Ensure the PDE works correctly and is not corrupted.
- **Availability of PDEs** - Ensure that the PDE can be accessed when required by an authorised user.
- **Confidentiality of PDEs** - Ensure that only authorised users can utilise the PDE to access stored data.
- **Availability of Data** - Ensure the data contained in the PDE can be accessed.
- **Integrity of Data** - Ensure the data in the PDE remains accurate.
- **Confidentiality of Data** - Ensure the data remains private.
- **Confidentiality of Revenue** - Ensure the privacy of payment details is maintained.
- **Availability of Revenue** - Ensure revenue can be obtained.
- **Non-repudiation of Revenue** - Ensure non-repudiation of revenue.

For this scenario we have chosen to focus and expand on the requirements involving the confidentiality of the data.

### Confidentiality of Data:

The confidentiality of data can be decomposed into looking separately at the data belonging to the user and the data belonging to a third party. The figure below shows this decomposition.

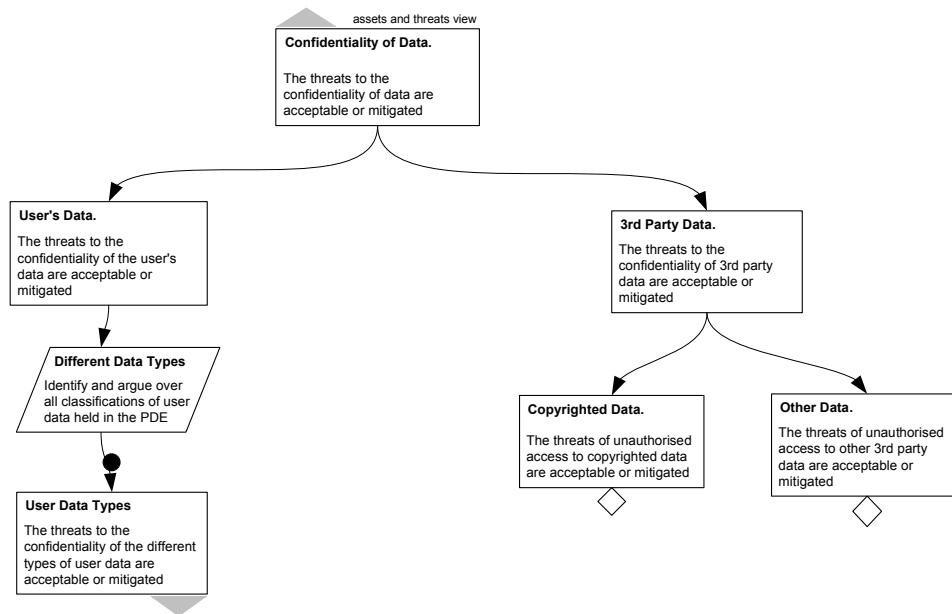


Figure 11: Scenario 2 - Confidentiality of Data

- **User's Data** - The threats to the confidentiality of the user's data are acceptable or mitigated.

User's data can further be split into the different types of user data stored and transmitted in the PDE, for example a personal address book and device configuration data. Hence we have a strategy to identify all the different classifications of data and argue over each of them:

**Different Data Types** - Identify and argue over all classifications of user data held in the PDE.

This leads to multiple sub-goals, one for each of the different types of user data.

- **User Data Types** - The threats to the confidentiality of the different types of user data are acceptable or mitigated.

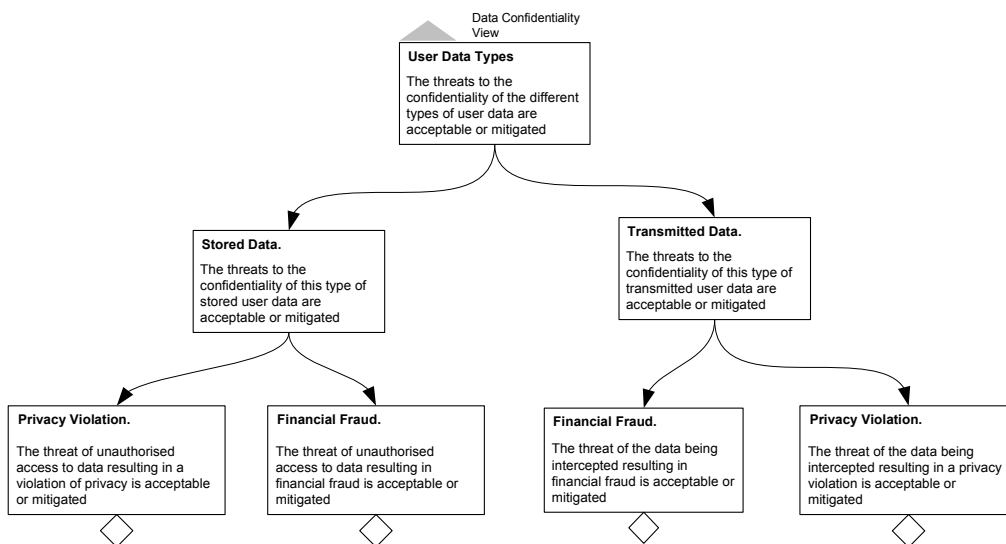


Figure 12: Scenario 2 - User Data

From a User's perspective there will be a demand for PDEs that prevent unauthorised cyber access to the information both stored in the PDEs and transmitted through it.

Thus, for each different type of user data we now consider the data stored on the PDE and the data transmitted through the PDE, resulting in the following sub-requirements:

- \* **Stored Data** - The threats to the confidentiality of stored data are acceptable or mitigated.

The data stored in the PDE not only includes personal information relating to preferences etc, but also financial data required to enable payments for services to be made. Depending on the type of data being stored, there could be the risk of financial fraud and/or a violation of privacy. This results in the following goals:

- **Privacy Violation** - The threat of unauthorised access to data resulting in a violation of privacy is acceptable or mitigated.
- **Financial Fraud** - The threat of unauthorised access to data resulting in financial fraud is acceptable or mitigated

- \* **Transmitted Data** - The threats to the confidentiality of transmitted user data are acceptable or mitigated.

Since the data transmitted around the PDE can be of a personal and/or financial nature, this requirement is decomposed into similar sub-requirements:

- **Privacy Violation** - The threat of the interception of data resulting in a violation of privacy is acceptable or mitigated.
- **Financial Fraud** - The threat of the interception of data resulting in financial fraud is acceptable or mitigated

- **3rd Party Data** - The threats to the confidentiality of third party data are acceptable or mitigated.

Third Party data can further be split into two different types, namely copyrighted data and other data that belongs to third parties but isn't copyrighted. Hence the following requirements:

- **Copyrighted Data** - The threats of unauthorised access to copyrighted data are acceptable or mitigated. This is likely to have a higher impact than on other data.
- **Other Data** - The threats of unauthorised access to other 3rd party data are acceptable or mitigated

### 4.3 Generating Evidence / Assurance Requirements

The table below describes a range of assets. Taking a simplistic view of these assets, their value (as implied by the impact of a security incident) can be rated in terms of the importance of confidentiality (C), integrity (I) and availability (A) as in the following table. The final column of the table provides an illustrative commentary on the threats, vulnerabilities and risks associated with these assets.

Asset	C	I	A	Threats/Risks
ICT devices	L	H	M-H	Theft, Loss, Tampering, Malfunction
PDE OS software	L-H	H	H	Planting of backdoors, bots, etc; Corruption; Unauthorised access to device features and hosted software/data; Planting of intruder device in PDE
PDE App software	L-H	H	H	Planting of backdoors, and other malicious software; Corruption; Unauthorised access to hosted data
PDE config data	H	H	H	Corruption leading to denial of service; Unauthorised modification leading to planting of intruder device in PDE
PDE user data	H	H	H	User privacy violation; User financial fraud
PDE network traffic	H	H	H	User tracking and behaviour monitoring; Corruption leading to denial of service; Modification leading to unintended actions at the PDE OS or application levels

Since the technology to implement a PDE does not yet exist, the implementation details are not known. Hence the likelihood of the threats occurring cannot be measured since they will depend on the technology used and developed. Once the design of the PDE has been more fully developed, the likelihood and risk levels can be determined.

The branch of GSN that we explored in the GSN diagrams can be related to the "PDE user data" asset, shown in the table. Once the likelihood and risk levels have been calculated they can be linked to the requirements identified in the GSN. Looking at the asset "PDE user data" in the table shows that the impact of the threat is high for all three types. This would suggest that the associated risk level is also likely to be high and thus a high level of confidence will be required to show the risk has been mitigated or been reduced to an acceptable level.

## 5 Remote Monitoring of Health in the Home Scenario

Presented in this scenario is the use of pervasive computing technologies to enable the remote monitoring of patients in their home environment. The purpose of choosing this scenario is to explore the use of Goal Structured Notation (GSN) not only to discover the security implications of such a system, but also the safety considerations that would also need to be addressed, as well as attempting to identify possible gaps in technology that would need to be addressed to deliver this kind of solution.

The scenario envisages the use of pervasive computing and wireless technologies in the home to support the delivery of effective care for the elderly and outpatients in a residential setting. A patient's mobility, vital life signs, drug use and nutrition levels can be tracked and measured by sensors in the home. This information can then be transmitted to a remote monitoring control centre for analysis. In turn this monitoring control centre can issue alerts to Trusts and Carers as necessary.

The use of telemedicine to enable patients to remain in their own homes for longer than would otherwise be the case has a number of potential advantages. For the patient it may provide a more congenial and 'almost normal' mode of living. For the local Health Trust it may deliver cost benefits and reduce demand on hospital beds. For society at large it may be seen as reflecting a caring patient-centric view of health service delivery and as a way of limiting one source of additional financial demands from health services.

The use of pervasive computing, sensor networks and wireless network technologies offer a range of new opportunities for the design of more versatile and capable telemedicine systems. These have been investigated by a number of research projects, such as the EU Mobi-Health project and work undertaken by NASA in the USA [1, 3]. Such projects provide pointers to the ways in which new technologies can be deployed to provide more versatile and capable support the patients in a residential setting. Other centres within the Next Wave programme are also investigating applications of this nature, see [www.dticareinthecommunity.com](http://www.dticareinthecommunity.com) and [www.ubicare.org/index.shtml](http://www.ubicare.org/index.shtml).

### 5.1 Scenario overview

A local health authority has an urgent requirement to deliver more health services direct to patients in their homes. They have identified the set of frail patients as those they wish to focus on initially. This is because the authority has identified pervasive computing technologies as a mechanism for remote monitoring of patient's health. In the case of frail and perhaps elderly people:

- such patients find it more difficult to travel to health centres,
- such patients would benefit from continuous monitoring of health since it may provide earlier warnings of deterioration,
- remote monitoring of health would enable patients to remain in their own homes for longer, as a pose to being in a hospital bed solely for observation purposes.

The authority will initially begin by placing various sensors in patients homes which will enable the health service to monitor:

- mobility of patients,
- drug usage of patients,
- nutrition levels of patients,
- vital life signs of patients.

The scenario is illustrated in Figure 13. The sensors will return all data to a central health database where the information will be processed. The system will automatically inform the ambulance authority, the patient's GP or other chosen support provider (such as family), should immediate action be required. The means of communicating the data from the home to the database will be chosen in response to information security requirements. The sensors will communicate data to a central hub/gateway within the home using some form of wireless communications.

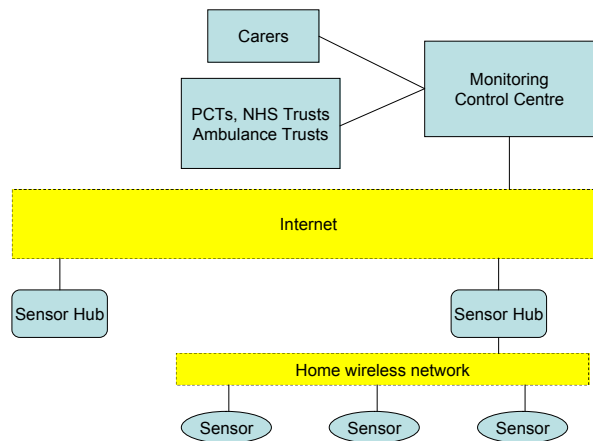


Figure 13: Operational Monitoring Scenario

The information stored on the monitoring database must be accessible to relevant UK health workers on demand, where ever they may be in the country. This must include information delivery to mobile devices.

## 5.2 Business Security and Safety Requirements

In this scenario we assume that the NHS has awarded a contract to a developer to develop the system. The system requirements are derived by the developer in cooperation with the NHS, so the requirements represent the views of the developer, but also include the NHS perspective.

In this scenario there is a clear safety requirement. If the system fails it could result in harm to human health and could cause a patient to die. However, it will be shown that the same process can be used and that there are no significant differences to approaches taken in the other scenarios.

A system described in scenario 3 could include complex functionality. For instance the system could learn from patient behaviour such as patterns of activity. This information could be used to detect changes that may indicate a change in health. However, such a system would have complex requirements, so we have constrained the system to a simple monitoring system where the outputs of sensors are fed to a monitoring system that displays and records patient sensor data for carers to monitor, alerting carers when preset thresholds are exceeded.

For the monitoring healthcare system described, there are several different elements of the system, the requirements of which need to be understood. These include the equipment components working correctly and reliably and the secure transmission of the data to the main control centre. Once again the risks associated with threats to the requirements not being fulfilled need to be assessed and managed appropriately.

The top-level template again applies (figure 2), illustrating the high level requirements of the system. The uppermost business requirement is for the system to provide adequate information security and safety. The meaning of adequate is again influenced by financial and commercial factors, considered as the context within which the technology needs to be developed. For this scenario, there is also a clinical context that influences the meaning of adequate.

- **Top Level Goal** - All information security and safety requirements should be adequately fulfilled

- **Top Level Contexts** - Financial Context, Commercial Context, Clinical Context
- **Financial Context** - As with the two previous scenarios, the company providing the monitoring service must satisfy its own financial requirements. In the development of the requirements of the technology, the company must bear in mind research, development, setup and running cost levels, revenue targets, and consider whether the technology is financially viable.
- **Commercial Context** - The commercial requirements of the company must also be taken into consideration, such as maintaining the company reputation and the needs of the health authority and its patients.
- **Clinical Context** - The system will be developed to meet clinical needs. Clinicians will have expectations of the system capability and levels of performance. Clinicians may also be responsible for the acceptance of the system.

The top-level goal is decomposed into two sub-requirements, once again illustrated on the top-level template; namely legal requirements and commercial requirements. The commercial requirements once again relate to ensuring that the delivery of the service is assured, whilst the legal requirements indicate the need to comply with certain laws and regulations.

- **Legal Requirements** - All relevant legal requirements must be complied with.
- **Commercial Requirements** - Ensure the delivery of the product/service is assured.

### **5.2.1 Legal Requirements**

Although not all of the laws, regulations and directives listed in the template may apply, they should always be considered, with requirements being generated if relevant. Because of the nature of this scenario, laws relating to Health and Safety and medical regulations also need to be considered, with the related ones generating requirements as appropriate and the goals for those laws and regulations being expanded as needed.

### **5.2.2 Commercial Requirements**

As with the previous scenarios, when deciding what the commercial requirements of the system are it is constructive to begin by thinking about the various assets that need to be considered and what non-functional properties about them are required,. Thus, a strategy to identify all assets and the threats to Confidentiality, Integrity, Availability and Non-repudiation for each of them, results.

- **Identify Assets and Threats Strategy** - Identify all assets and identify the threats to the Confidentiality, Integrity, Availability and Non-repudiation for each of them.

For this scenario, the assets are identified to be the data, the care resources such as the carers and the ambulance service, and the system software. The threats to the confidentiality, integrity, availability and non-repudiation of each of these assets need to be considered. For data, there are threats to its confidentiality, integrity and availability, for care resources, its availability is threatened and for the system software there are threats to its integrity and availability. The fidelity of the sensors monitoring the patient are not considered as they are deemed out-of-scope. They are expected to report in a certain way, but we are not concerned about how they arrive at the data they report.

The following GSN diagram shows the assets and threats associated with this scenario.

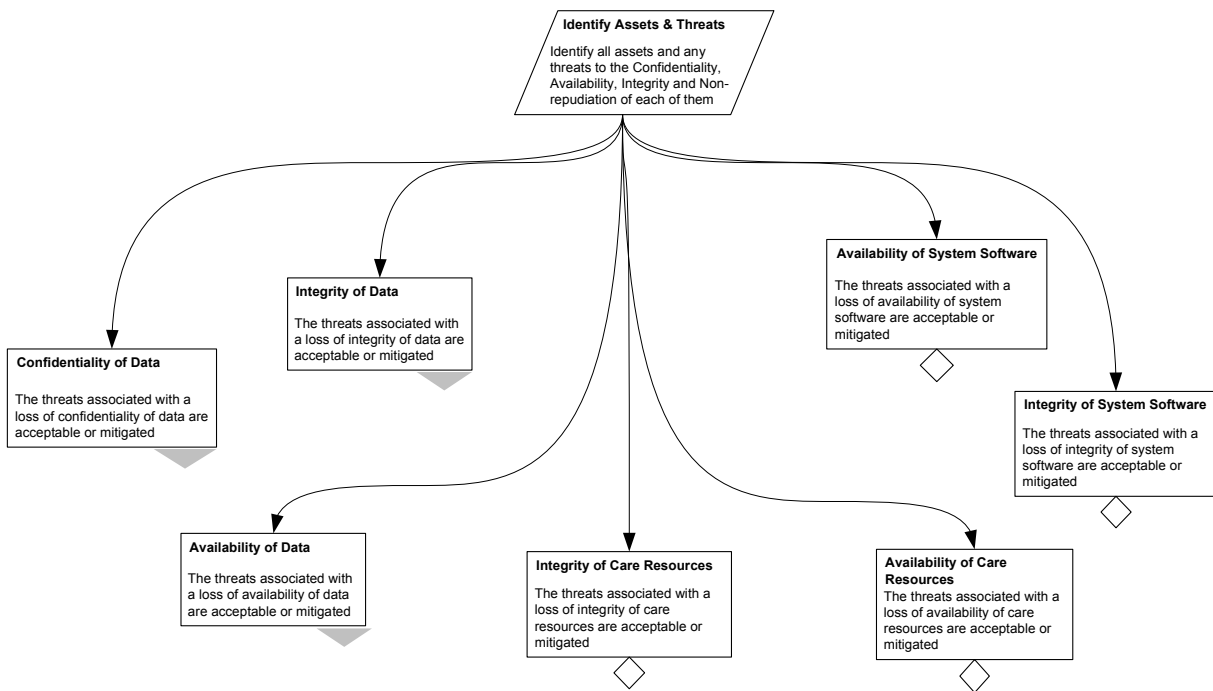


Figure 14: Scenario 3 - Assets and Threats

Thus, the commercial requirements can be decomposed into the following sub-requirements:

- **Confidentiality of Data** - Ensure that the privacy of the data is maintained.
- **Integrity of Data** - Ensure the accuracy of the data.
- **Availability of Data** - Ensure the data can be accessed by carers.
- **Availability of Care Resources** - Ensure the carers and other resources are available .
- **Integrity of Care Resources** - Ensure the care resources are able to understand and use the system.
- **Integrity of System Software** - Ensure the software works correctly.
- **Availability of System Software** - Ensure the software works when required.

Unlike the previous two, this scenario has safety related concerns, because it involves the care and health of patients, which will have to be addressed in the requirements. Therefore, this scenario adds an added dimension to our use of GSN, about where safety requirements may manifest. For this scenario, we have concentrated on the threats to the Confidentiality, Integrity and Availability (CIA) of the Data asset, in particular personal data relating to the patient, to show how safety requirements and security requirements can intermingle.

#### **Confidentiality of Data:**

The confidentiality of data can be split up into looking at the confidentiality of the data held about the patient and the confidentiality of the data relating to the system itself.

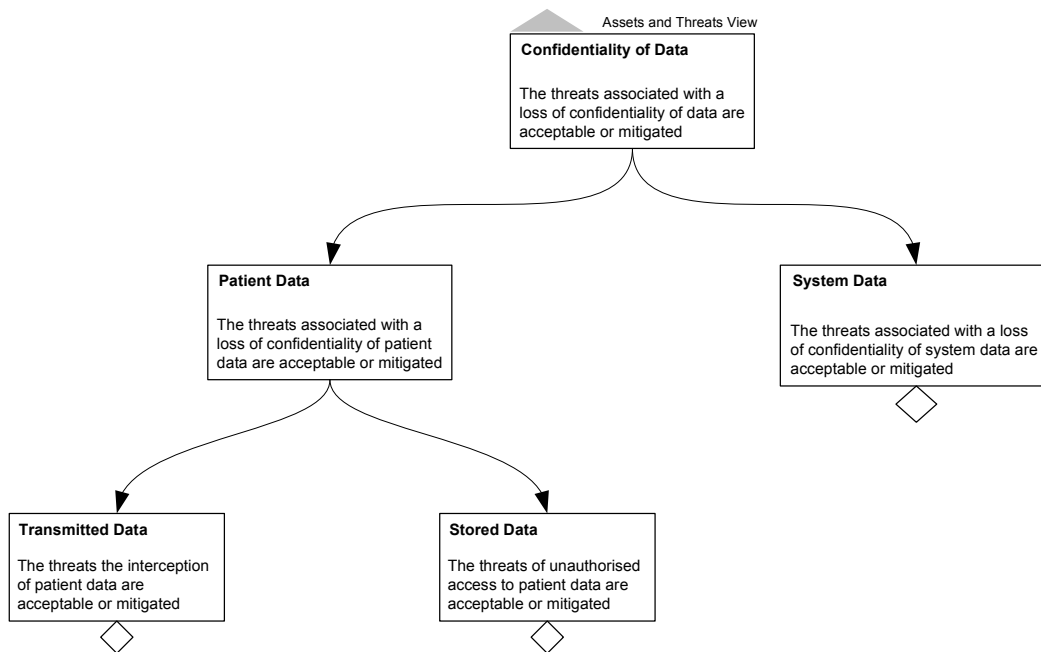


Figure 15: Scenario 3 - Confidentiality of Data

- **Patient Data** - The threats associated with the loss of confidentiality of patient data are acceptable or mitigated

The handling of patient data is a complex issue and may not be entirely covered by the Data Protection Act (DPA). Patient data relates not only to the data the sensors produce but also to any other data stored in the system about the patient. Some of the data relating to the patient, such as their temperature and drug intake, may not be covered by the DPA. Hence, this requirement refers to the data that the patient may want kept confidential, but which is not classed as personal data as defined by the Act.

Patient data can be split into stored and transmitted data, resulting in the following requirements:

- **Transmitted Data** - The threats associated with the interception of patient data are acceptable or mitigated
- **Stored Data** - The threats associated with the unauthorised access to patient data are acceptable or mitigated
- **System Data** - The threats associated with the loss of confidentiality of the system data are acceptable or mitigated

### Integrity of Data:

The integrity of data can again be split up into looking at the integrity of the data held about the patient and of the data relating to the system itself.

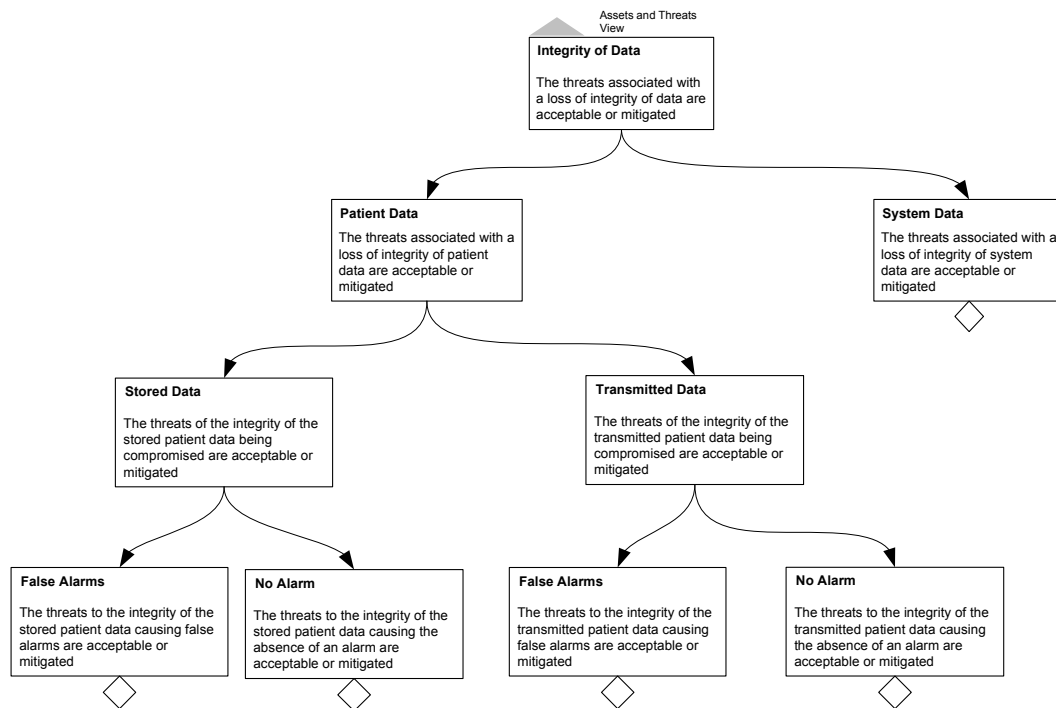


Figure 16: Scenario 3 - Integrity of Data

- **Patient Data** - The threats associated with the loss of the integrity of patient data are acceptable or mitigated

Corruption or loss of patient data can result in a reduction of system performance and harm to the patient. Patient data can be split into stored and transmitted data. Sensor data is transmitted to the monitoring and control centre and patient data, such as patient records, are stored in the monitoring and control centre.

- **Stored Data** - The threats associated with the loss of the integrity of stored patient data are acceptable or mitigated

Patient health care decision will not only be based on transmitted data, but also on stored data such as patient records. Carers will use the stored data and transmitted data to determine the patient's health care needs. The integrity of the stored data must be maintained.

- \* **False Alarms** - The threats associated with the loss of the integrity of stored patient data resulting in false alarms are acceptable or mitigated  
The integrity of the information must be high enough to reduce false alarms to an acceptable level.
- \* **No Alarms** - The threats associated with the loss of the integrity of stored patient data resulting in no alarms are acceptable or mitigated  
The integrity of stored data must be high enough to alert carers of a need for help in time.

This second requirement conflicts with a need to avoid false alarms. False alarms are not directly hazardous. However, false alarms could have two indirectly hazardous outcomes. Attending a false call out could cause resources to be diverted from a genuine call out and frequent false call outs could adversely affect carers' response to alarms.

Stored data must be accurate. The information must be of high enough quality to allow carers to recognise a need for help in time and messages sent to the patient must be correct and clear.

– **Transmitted Data** - The threats associated with the loss of the integrity of transmitted patient data are acceptable or mitigated

\* **False Alarms** - The threats associated with the loss of the integrity of transmitted patient data resulting in false alarms are acceptable or mitigated.

The integrity of the information must be high enough to reduce false alarms to an acceptable level.

Messages must be accurate. The information must be of high enough quality to allow carers to recognise a need for help in time and messages sent to the patient must be correct and clear.

\* **No Alarms** - The threats associated with the loss of the integrity of transmitted patient data resulting in no alarms are acceptable or mitigated

The integrity of the information must be high enough to alert carers of a need for help in time.

This conflicts with a need to avoid false alarms. False alarms are not directly hazardous. However, false alarms could have two indirectly hazardous outcomes. Attending a false call out could cause resources to be diverted from a genuine call out. Frequent false call outs could adversely affect carers' response to alarms.

• **System Data** - The threats associated with the loss of the integrity of patient data are acceptable or mitigated

Corruption or loss of system data can result in a reduction of system performance and harm to the patient. Threats to the integrity of system data should be adequately mitigated.

**Availability of Data:**

The availability of data can be split up into the integrity of the data held about the patient and data relating to the system.

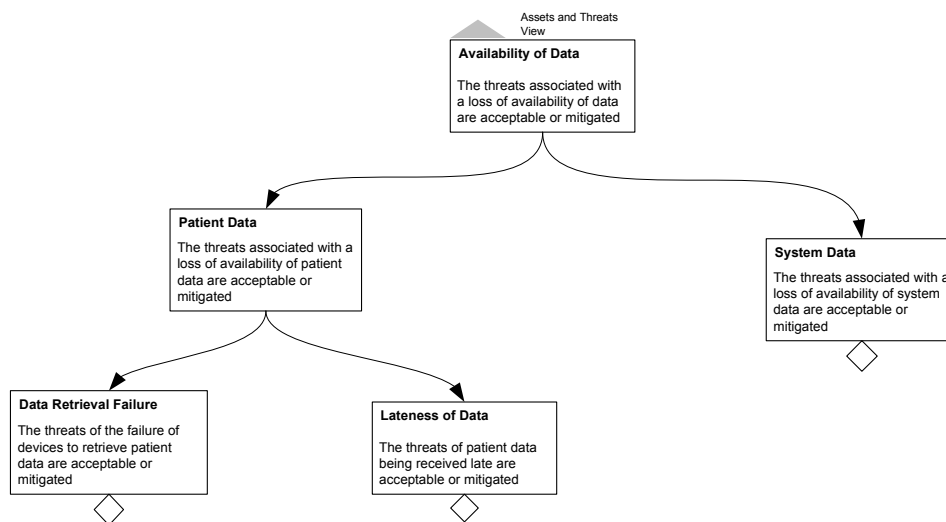


Figure 17: Scenario 3 - Availability of Data

• **Patient Data** - The threats associated with the loss of the availability of patient data are acceptable or mitigated.

Loss of patient data can result in a reduction of system performance and harm to the patient.

– **Data Retrieval Failure** - The threats associated with the loss of the availability of patient data resulting from a data retrieval failure are acceptable or mitigated.

Data must be delivered and the system should be acceptably reliable. If the system is known to have failed, alternative health care could be provided. So the system should not fail in an undetectable way.

- **Lateness of Data** - The threats associated with the loss of the availability of patient data resulting from data not being received on time are acceptable or mitigated.

Data should be given within accepted time limits. The monitoring must give timely information.

- **System Data** - Loss of system data can result in a reduction of system performance and harm to the patient. Threats to the availability of system data should be adequately mitigated.

#### **Availability of Care Resources:**

The implementation of remote health care monitoring would change the way in which health care is provided. More patients will be treated at home. In addition, this is likely to result in a redirection of health care resources. With many patients being cared for in their own homes using the system it is unlikely that there would be enough resources to cope with a wide spread system failure. The system must be reliable, but it is unlikely to be perfect so the health care system must be able to cope with an anticipated level of failures and false alarms. This requirement does not come directly from the system, but from the way in which the system changes the environment in which it operates.

#### **Integrity of Care Resources:**

Carers must have an accurate understanding of the system performance and limitations. When the system is working as expected it could still fail to meet the patient's health care needs because the patient's needs are too demanding to be adequately cared for by the system operating within its specification. This could be that the monitoring cannot monitor the patient's condition or that the response to a change is not adequately timely. The patient's carer would have to make a decision about the adequacy of the system for a particular patient.

### **5.3 Generating Evidence / Assurance Requirements**

The table below describes a range of incidents and a measurement of the risk associated with them (normally output from a standard risk assessment).

Incident	Impact	Likelihood	Measure of Risk
Intermittent interruption of monitoring	L (localised)	M (probably accidental)	M (-)
	M (general)	L (probably accidental)	M (-)
Prolonged interruption of monitoring	M (localised)	L (unless malicious intent)	M (-)
	H (general)	M (control centre attack)	M (+)
Misleading monitoring measurements	H (localised)	L (unless malicious intent)	M-H
	VH (general)	VL (many attacks needed)	M (but extreme event)
Interference with patient self treatment regime	H (localised)	L (unless malicious intent)	M-H
	VH (general)	VL (many attacks needed)	M (but extreme event)
Patient privacy compromise	M (localised)	M (local or centre attack)	M
	VH (general)	M (control centre attack)	H

Many of these sources of vulnerability and (consequentially) attack opportunities are common to any analysis of security risks. The less common vulnerabilities that are specific to this telemedicine scenario are those concerning the design and operation of sensor networks in the home. These raise security issues in the following areas:

- The protection of wearable sensor networks from manipulation by an attacker so as to interfere with their operation or to introduce 'alien' sensors that can be used as conduits for interference or interception attacks
- The protection of item-based sensor networks (e.g. an instrumented drugs dispensing cabinet) from manipulation by an attacker so as to interfere with their operation or to introduce 'alien' sensors that can be used as conduits for interference or interception attacks
- The protection of house-based sensor networks (e.g. to monitor patient location and activity levels) from manipulation by an attacker so as to interfere with their operation or to introduce 'alien' sensors that can be used as conduits for interference or interception attacks
- The protection of the sensor hub and internetworking arrangements within the home from manipulation by an attacker so as to interfere with their operation or to introduce 'alien' sensor networks that can be used as conduits for interference or interception attacks.

Whilst this list of issues may appear repetitive it is significant as the practical engineering options for addressing these issues may vary. For instance, the functional capabilities of wearable sensor networks are likely to be extremely limited, possibly ruling out the use of techniques that are demanding in computational power or code storage capacity, such as strong encryption algorithms. Interestingly it has been suggested these limitations might turn out to be an advantage in some situations as they could reduce the ease of eavesdropping on very low power communications [2].

The risk assessment identifies and quantifies risks. This measure of risk can then be used to determine the criticality of system components and the degree of evidence required to show that the components performs as required. Some component failures could result in harm to patient health, so some of the evidence is needed to show that the system is safe.

**Comparison between Security and Safety Risk Assessments:**

The security assessment above identifies safety as a concern, but it does not address safety directly. A safety assessment would identify failures that are harmful to patients and then focus on ways in which those failures could occur. Initially this would be to identify safety requirements to be used by the developer and later to show that the safety risks have been adequately mitigated. This is necessary in order that developers and third parties such as regulators, courts of law, users and other interested parties can be convinced that safety has been adequately addressed. The need to be able to demonstrate to third parties that adequate care has been taken is specific to safety and comes out of the legal requirement including the need to show that best practice has been followed in the event that someone is harmed. There are key elements of safety risk management that differentiate it from security.

- Usually the only assets to be considered human life and the environment.
- There are safety processes that are well defined and widely followed (often prescribed).
- Risk targets are more strictly defined and are often expressed in probabilistic terms.

There is a synergy between safety and security risk management. Both analyse systems to identify threats, and then assess the risk level from the likelihood and impact of the threat. There are also differences between safety and security risk management. Unlike the system described in Scenario 3, traditional safety systems are closed and do not consider malicious or cyber threats. There are also differences in the way that risk is measured. Dependable systems such as the remote health care system described in scenario 3 require an approach that considers both safety and security.

## 6 Dynamic Risk Management

Levels of security and safety risk may change once the system is in use, and after the initial risk assessment. This could be due many factors, including: discovery of vulnerabilities in components; changing threat environment; unexpected system utilisation; unauthorised and ad-hoc changes to system configuration. The only practical approach to protecting against systems becoming less secure or safe is the development of a dynamic risk management policy and process; monitoring and re-assessment will have to be continuous and more precautionary, rather than reactive. The process must make it possible to quickly recognise a change in threat and the effect on the risk level to the system so that appropriate controls can be quickly put in place. For this to be successful there has to be a clear record of system vulnerabilities, threats, impact and a method to quickly re-assess the change in risk level. A Goal Structured Notation (GSN) argument would enable this, below we describe how our requirements methodology could be extended to enable this.

Having determined the security and evidence requirements of the system, with Step 5 solutions and implementations can then be chosen or developed with the view of meeting the identified requirements. Possible solutions may not only be in the form of technologies or products, but can also include managerial procedures and guidelines. Our methodology is extended to include in Step 5 the documentation of these solutions and the assurance evidence gathered for each component.

- Extend GSN security requirements diagram to include documentation of solutions utilised to meet security requirements, the evidence levels required to demonstrate solutions adequacy for purpose, and the actual type of evidence gathered.

Once sufficient solutions and evidence have been documented the GSN case is complete. The finished case documents: the contribution all system security and safety evidence requirements have on the overall security case of the system, and the solution chosen to meet the requirements and deliver the overall system goals.

The GSN security argument identifies system components that contribute to system risks. If the assessment of a component changes, or the system require evolution for *any* reason, the security case should be revisited and the extend of the change can be traced. The affect on system security can quickly be seen and reassessed. Importantly the GSN will identify everywhere that the affected component appears, so the overall affect of the change can be seen.

For example, an operating system (OS) could be used as a common component in a system. The GSN would identify every instance where this OS is used and has a security requirement. If a new vulnerability was identified in an OS then the change in risk across the whole system could be considered. This knowledge will enable system managers to make affective risk management decisions. The GSN for this is shown in Figure 18. From the GSN we can see that the goals A and B are reliant on the evidence from solution C. So if the evidence from C changes then both A and B have to be reassessed. As we know that only goals A and B are affected and exactly how they are reliant on C then the affect can be completely and efficiently assessed.

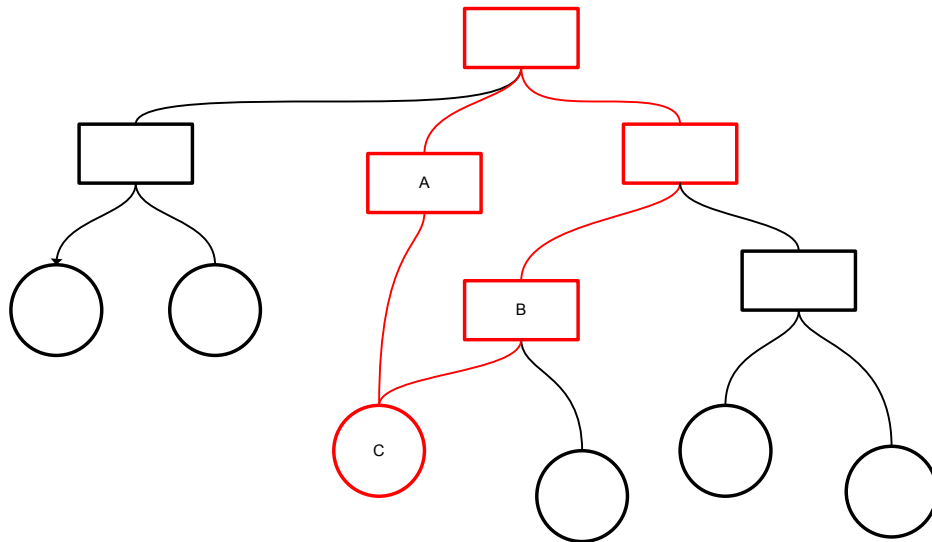


Figure 18: Affected Requirements due to change in Component Risk Assessment

The top level requirements could also change, for instance the nature of the business changes. Flowing down from the top level goal the affect on each goal can be considered until the affected solutions are identified and the new evidence requirements established as shown in Figure 19. When the top level goal changes then the GSN shows the child goals that are affected. This can be traced to the evidence that supports those goals. In this example the evidence in solutions F and G are affected and need to be reassessed.

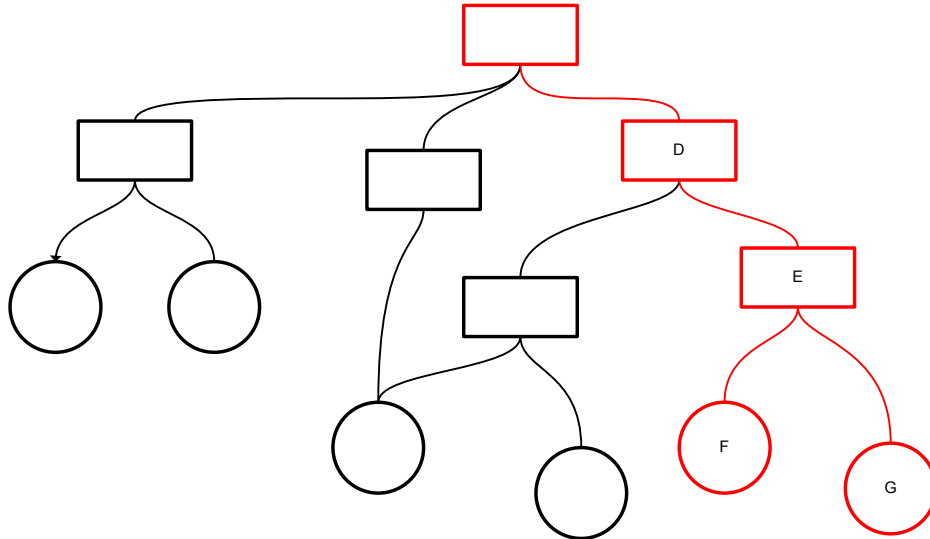


Figure 19: Affected Solutions and Requirements due to a change in the Top Level Requirement

## 7 Conclusions and Future Work

### 7.1 Results

We have presented a methodology for capturing information security requirements. The methodology is designed to:

- Support the decomposition of system security requirements to a component level, which supports solutioneering and procurement from third parties.
- Provide a notation which directly links the assessment of assets requiring protection, the risk to those assets and the resulting information security requirements of the system. Further, the security requirements are directly linked to the system components delivering the solution, and the assurance requirements made of components of the solution so demonstrating how the assurance requirements support the overall security solution.
- Provide a graphical presentation of the system security argument which is intuitive to use and easily scalable.
- Provide a method for efficiently assessing the impact of environmental change on the requirements, solutions and assurance methods for the entire system.

The methodology is easily repeatable with use of the template we have developed. The methodology also allows for re-use of components, minimising the overhead of assurance for evolving systems. We have demonstrated the applicability of the template by application to three scenarios; which together are designed to provide a mechanism for investigating a broad range of requirements applicable to many other applications. We have also discussed how the methodology may be extended to include systems with safety requirements in addition to security requirements. Finally, we have outlined how the methodology could be extended to facilitate dynamic risk management throughout a system's life-span.

### 7.2 Validation and gap analysis

Our current consideration of the scenarios is only partial, and so cannot be considered a validation of the methodology. They are also not deep enough to enable a technology and solution gap analysis, although we can already begin to predict where the problems might be. Our next stage in this research is to conduct a deeper validation which would support such a gap analysis.

### 7.3 Potential for tool support

The production of Goal Structured Notation (GSN) diagrams is currently supported by simple drawing tools. These tools could be extended to aid the production of security cases, and so make it easier for non-experts to employ the methodology.

Security cases contain many elements that have common structures and components. For instance, a common structure would be to argue that a component has Confidentiality, Integrity and Availability. Arguments that these properties are met are also likely to have common patterns. These and other reusable properties of GSN security cases could be supported within the tool as libraries of templates and strategies. The process of carrying out the security analysis could also be supported within a tool. For instance the analyst will have a mental check list of properties such as CIA that they will consider when they carry out the analysis. This process could be supported within the tool thus making the construction of the security argument more transparent and demonstrably complete.

Further, the GSN could be developed into a tool that manages the reassessment and dynamic risk management. The risk assessment could be built into the GSN, with the impact and likelihoods being included in the GSN so that the risk level can be automatically calculated. For instance when a new vulnerability is identified then this could be included in the GSN and the risk level recalculated.

In the long term the tool could exist on-line, monitoring changing threat environments reported in open source, such as the tracking of bugs in software. When a change to the threat environment occurs due to such open source information the tool could automatically record which parts of the security solution are impacted, and alert the person responsible for system security.

We do not expect to be able to develop any tool-support within the FORWARD project.

## References

- [1] Ec mobihealth project. <http://www.mobihealth.org>.
- [2] B. Cole. Pervasive computing undergoes a near-body connectivity experience. *IEEE Pervasive Computing Issue 4*, October-December 2004.
- [3] K.J. Liska et al. Keeping a beat on the heart. *IEEE Pervasive Computing Issue 4*, October-December 2004.
- [4] S. Creese M. Goldsmith R. Harrison A. Hood C. Pygott J. Roach W. Simmonds K. Azeem, P. Beechey and P. Whittaker. Analytical assessment of bluetooth security mechanisms. FORWARD Deliverable, [www.forward-project.org.uk](http://www.forward-project.org.uk), January 2004.
- [5] T. Kelly. Safety case management: A systematic approach. John Wiley and Sons Ltd, May 2004.

## List of Abbreviations

**CIA** Confidentiality, Integrity and Availability

**DPA** Data Protection Act

**EAL** Evaluation Assurance Level

**GSN** Goal Structured Notation

**IP** Intellectual Property

**OS** operating system

**PDE** Personal Digital Environment

**SIL** Safety Integrity Level