Dependability Requirements of Large-Scale Information Infrastructures

A Case Study from the Health Care Sector

2000

EUROPEAN COMMISSION
JOINT RESEARCH CENTRE
Institute for Systems, Informatics and Safety

EUR 19642 EN

EUR 19642 EN

Printed in Italy

Title: Dependability requirements of large-scale information infrastructures. A case study from the Health Care sector

Abstract: This report seeks to acquire and promote a better understanding of the dependability requirements emanating from applications of large-scale information infrastructures. To accomplish this aim, a case study from the health care sector is performed in collaboration with a large health care enterprise.

Date: 26/05/2000

Authors: Marc Wilikens, Tom Jackson
Joint Research Centre (JRC) – TP 210
21020 Ispra (VA) – Italy
Tel: +39 332 789737, Fax: +39 332 789576
Marc.Wilikens@jrc.it

Alberto Sanna
Scientific Institute Hospital San Raffaele
Laboratory Medicine Dept.
Via Olgettina, 60
20132 Milano Italy
alberto.sanna@hsr.it

Distribution: Unlimited

TABLE OF CONTENTS

1 Introduction

1.1 Purpose

This report seeks to acquire and promote a better understanding of the dependability requirements emanating from applications of large-scale information infrastructures. An important application area depending on such infrastructures is to be found in health care. The characterisation of requirements is achieved by means of a case study from the health care sector and is performed in collaboration with a large health care enterprise.

1.2 Rationale

A number of important trends can be found in emerging health care systems. These include:

- The promotion of remote health care monitoring and working practices by exploiting new telematics services.
- The information and knowledge intensive nature of modern health services and the fact that health care value is increasingly produced by means of interaction between a variety of processes and stakeholders within virtual health care enterprises.
- The promotion by various European governments of the use of electronic mobile media in health. For instance, the use of smart cards in Germany for billing, in France for carrying health data and the use of a pan European health passport for emergency medical information.

Dependability issues in health are driven by the need for patient safety and privacy whilst assuring highly efficient and available health services within strict budgetary constraints. The above trends seriously impact dependability issues because:

- There is a unprecedented dependence in any healthcare activity on information flow, both for efficiency and quality purposes.
- Health data are handled and shared in large-scale distributed and interconnected systems that cross the borders of the traditional health care enterprise.
- The large number of stakeholders and the complexity of systems involved, cause heterogeneity of dependability requirements and strong interactions between system requirements both within and between the different layers of abstraction of these systems.

1.3 Approach

We propose a harmonised approach to requirements characterisation, starting from generic stakeholder requirements that are rooted in risk evaluation. To satisfy these aims, we first describe in chapter 2 the new health system context that influences dependability. In chapter 3, we elaborate on stakeholder requirements, risks, threats and vulnerabilities within the health domain. In chapter 4, we describe a generalised set of dependability attributes together with a requirements elicitation process necessary for specifying user dependability requirements in health care.

2 The Health System context

2.1 Vision: "patient centred care"

The healthcare sector is the largest single service sector, accounting for approximately 500 billion ECU (600 billion $) in the European Union (approximately 9% of the GDP). The

healthcare sector is currently undergoing a paradigm shift from a healthcare system centred approach to a patient (citizen) centred care in which emphasis is placed on continuity of services for supporting health promotion and maintenance. The new paradigm implies a shift from a centralised approach to one with distributed responsibilities in which an informed citizen needs easy access to health care at any time and place and in which other health care stakeholders are responsible for the continuity of services within a certain region. In this context, Internet and IT are playing an increasingly important role in the delivery of services. In the USA alone, the health industry spent between $ 12 billion and $ 16 billion on IT in 1996. Information and communications infrastructures implement electronic medical records, support information distribution and sharing between health promotion, primary health care, hospital services, home care and other relevant service mechanisms for patient care and tele-medicine provides remote health care.

A number of important business, legal and technological drivers shaping dependability are described in the following sections.

2.2 *Business drivers*

The health and medical sector has scope for major reforms of its working practices through the adoption of distributed IT products and services. Main drivers include:

2.2.1Cost and social sustainability

In recent years, the need for social sustainability of the health care system has forced health services to introduce quality improvement in order to maximise the benefit of finite resources.

2.2.2 Information and knowledge intensive

Health care provision is highly dependent on information and knowledge management for two main reasons: i) The universality of healthcare service and ii) The complexity of healthcare delivery. Universality and complexity of healthcare delivery result in a vast and distributed healthcare system, composed of sub-systems/enterprises that range from doctor's offices and small labs to huge university hospital settings and service management systems (e.g., insurance companies, regulatory bodies).

Interactive Performance: Health care service is performed by a variety of clinical and non-clinical interactions between health care providers and beneficiaries. Therefore, at the point of interaction (e.g. the patient), the availability of context dependant information is crucial for service provision.

Universal electronic patient record: One of the most fundamental changes, currently being introduced, is the transfer of patient records onto electronic databases, and the demise of records maintained within paper files. One scenario being proposed is the move towards a universal electronic patient record. This scenario implies electronically stored health information about one individual which is uniquely identified (e.g. by means of centralised databases for health records, either at regional or national level). This entails capturing, storing, retrieving and transmitting patient-specific health care data, including clinical, administrative and biographical data. The move to electronic data management also opens up the potential for much wider exploitation of IT.

2.2.3 Remote health care

Patients will be able to consult their General Practitioner (GP) or consultant remotely using telematics services over the communications infrastructures such as the Internet. Features such as real-time video conferencing, expert-systems diagnosis and on-line analysis (for

example, real-time monitoring of dialysis treatment) could be made available. In the longer term, it is foreseeable that operations may also be carried out remotely. For example, in the US trials are currently being performed on a remote-control robot for heart by-pass surgery [1]. A surgeon, via hand controls and large TV monitors, controls the robot. Potentially, the surgeon could be remotely linked to the operation, over long distances, via the Internet or dedicated phone line connections.

2.3 Legal drivers

Personally identifiable health data are exchanged globally on a daily basis by governments, pharmaceutical firms, health care enterprises and others. In October 1998, the European Union privacy directive on "protection of individuals with regard to processing of personal data and on the free movement of such data" came into effect [2]. The resulting legislation will have important implications for privacy in general and movement of health data in particular. The Directive covers all personally identifiable data processed in Europe, regardless of the data origin of the data or the data subject. The two important issues in the Directive are first that for the processing of data that are personally identifiable, consent from the data subject is generally required. Second, the transfer of data to third countries may take place only if the recipient country assures an adequate level of privacy protection. In respect of the sector specific nature of data privacy (e.g. health research), specific codes of conduct are promoted.

2.4 Technological and system drivers

2.4.1 Distributed System Architecture

The Internet has become an important interactive communication infrastructure for both medical professionals and health consumers. Intranets and Extranets are being tapped by many hospitals for sharing medical information and collaboration in-house within Health Care Enterprises or outside within products supply chains (e.g. pharmaceutical industries, clinical equipment providers). The move towards distributed systems on top of "open" communications infrastructures poses new types of risks. Therefore, on top of these infrastructures, schemes including certificates, digital signatures and encryption are being investigated in the health domain for increasing trust in transactions. Figure 1 reflects a typical future health care architectural framework. It includes the main components and stakeholders of a distributed networked health system implemented on a public communications infrastructure. The various applications of IT in health care are generally referred to as Health Care Information Systems (HCIS). These could include centralised databases for keeping some of the Citizen's health records (e.g. within government organisations). Within Health Care Enterprises or individual hospitals, hospital information systems are being implemented widely. Components within such a system might include an admission/discharge system, scheduling and registration, electronic patient record, laboratory information system, pharmacy system and a financial management system. At the clinical level, applications providing decision support to doctors and robotics providing surgical support to surgeons are being developed. Tele-medicine, which connects geographically dispersed health care facilities via telecommunications, is now used to access imaging patient records and to perform remote clinical diagnosis and surgery. Also home-care will increasingly rely on technological innovation, including telematics. Hospital infrastructures could also be linked to emergency and Government infrastructures for the electronic distribution and management of public health information (regulations, health care statistics, etc.) as well as contingency plans for crisis situations (natural disasters, large scale accidents, war scenario).

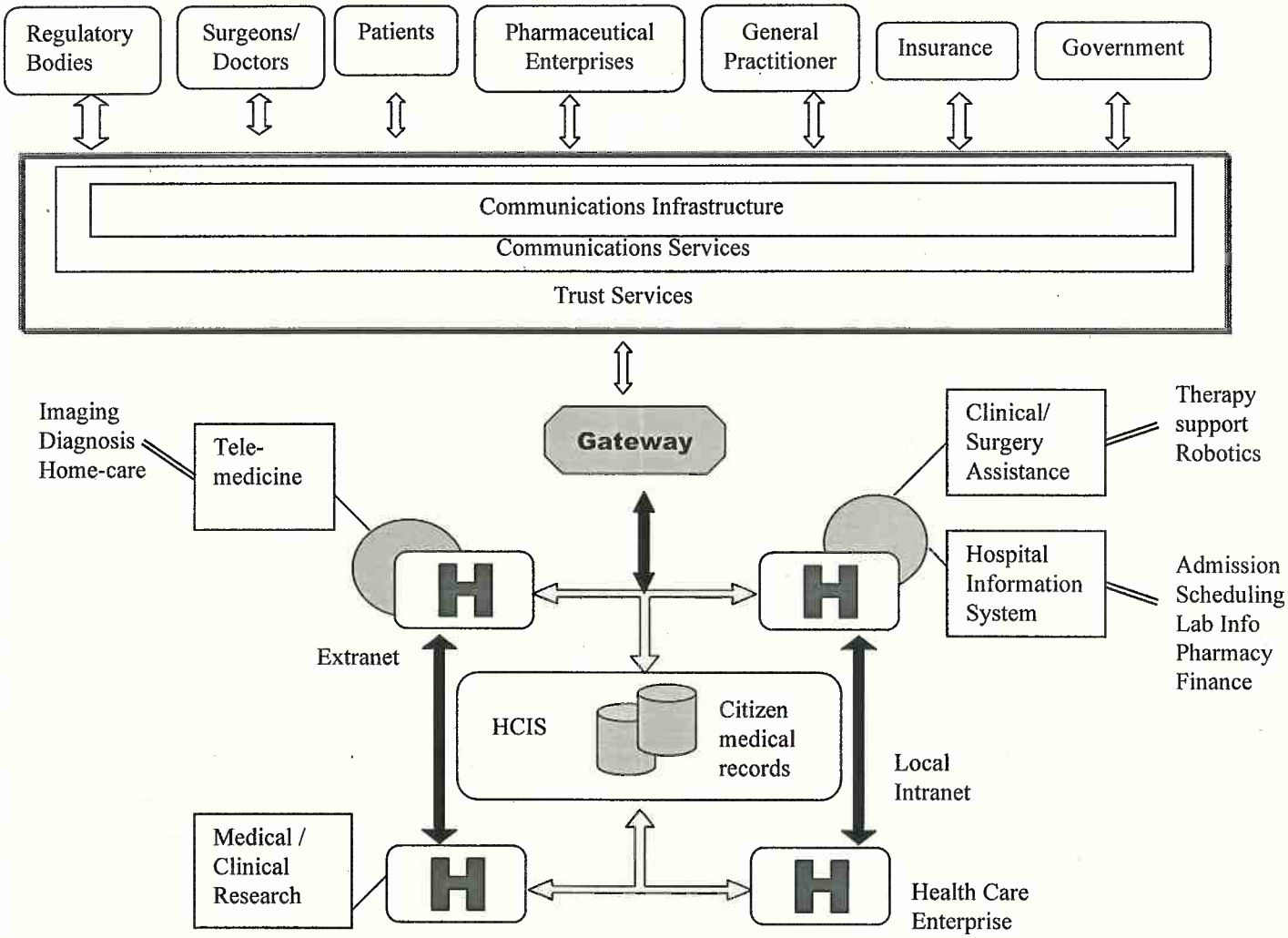


Figure 1: Health care system architecture

2.4.2 Business process integration in virtual enterprises

Communications infrastructures allow the integration on a wider scale of:

- Internal hospital processes both clinical and non-clinical;
- Other business processes involved in health care such as pharmaceutical industries, insurance and government administrations giving place to virtual healthcare service systems or virtual enterprises. Already, centralised hospital databases are linked to pharmaceutical suppliers directly, for the automatic control and supply of drug inventory.

A scenario for business processes integration found in a modern health care environment is schematised in the figure 2.

The Citizen / patient flow (top horizontal part of the figure) includes a set of processes before a citizen is admitted in the Health care enterprise as a patient.

The Health Care Enterprise (HCE) is a major component in the health care system, and consists of a set of processes including clinical activities on the patient (therapeutic, preventive), clinical support services (e.g. hospital pharmacy, laboratory, etc) and non-clinical support services including logistics and information flow support.

On the supplier side (left vertical part of the figure), pharmaceutical companies and distributors, non-capital medical/surgical goods suppliers and non-capital diagnostic goods suppliers feed into the HCE by providing products, devices and related information.

In such a scenario, healthcare service is produced by means of interactions among enterprises and within enterprises in a number of hierarchical services delivered on a customer/provider basis and managed with a contract/subcontract model between parts. A unique healthcare macro-activity, delivered to the main customer - the Patient - is but the tip of the iceberg of a complex set of electronic and non-electronic processes. Increased complexity also increases the risk of failure of critical processes. Critical electronic processes predominantly consist of both transactions (e.g. financial, medical data transfer) and interactions with patient related information objects at the point of care (e.g. control of therapy information). Some of the techniques deployed or under development in the e-commerce domain for secure transaction management are therefore also of relevance in health care.

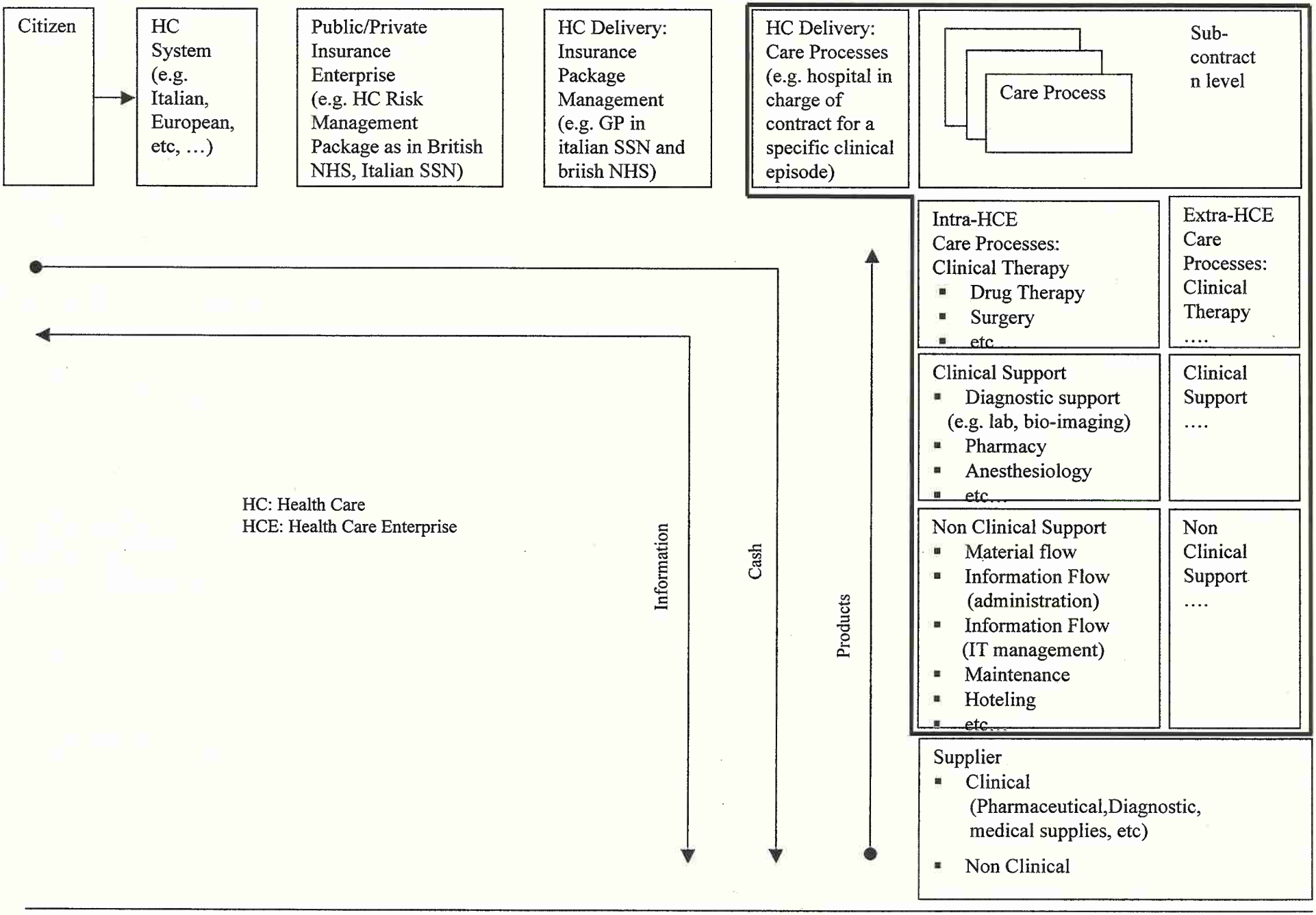
2.4.3 Legacy systems

An important category of problems in health care is related to the use of a large diversity of legacy systems. However, legacy systems were not designed with the idea of directly connecting to corresponding systems in other companies by means of public infrastructures. When organisations join a larger infrastructure for collaboration, they typically need to share information in a selective way. Indeed, companies need assurance that, upon integrating into an information sharing environment, the security policies of their local systems can still be enforced.

2.4.4 Organisational factors

Healthcare is a human-machine system i.e. a technological organisation, in which human, technical and organisational factors interact in order to deliver healthcare. After a massive introduction of IT, a patient-centred vision of healthcare delivery, even more than before, calls for the evaluation of human performance within the more general context of system performance in order to manage risk and preserve patient safety.

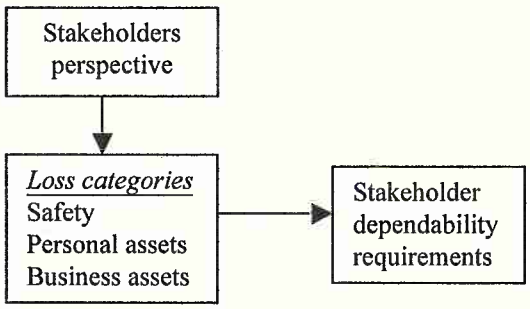
Figure 2: Health Care Business Process Framework



3 Dependability risks

3.1 Stakeholders requirements

The deployment of distributed and interconnected information systems in the health sector on top of public infrastructures, such as the Internet, will bring clear and obvious benefits to the stakeholders in health care but presents several dependability concerns. These dependability concerns vary with the stakeholder perspective. We consider as stakeholder dependability requirements the stakeholder perspectives on the losses (risks) to which they are potentially subjected. Three generic categories of losses are safety (e.g. loss of life), personal assets (e.g. privacy invasion, lack of personal data integrity) and business assets (e.g. economic loss due to business process unavailability).



Important stakeholders in health care and examples of stakeholder requirements include:

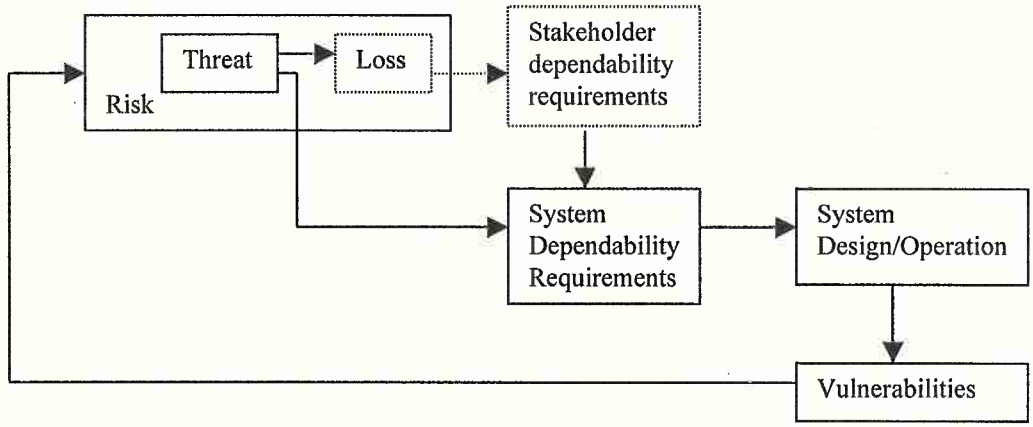
- Patient/Citizen:
  - To preserve patient safety, meaning avoidance of personal injury and pathologies due to adverse clinical events.
  - To preserve privacy of personal information.
  - To receive high levels of quality of health care.
- Health Care provider:
  - To ensure confidentiality of the relationship with the patient in accordance with ethical terms.
  - To ensure quality of the service in accordance with contractual terms.
  - High availability in all conditions.
- Internal and external logistics suppliers:
  - To provide products, devices, services and up-to-date product information in a timely fashion.
  - Ability to supply peak demands.
- Internal and external infrastructure service providers:
  - To support security of information flow. This applies to information stored on health systems as well as for transmitted information. If Internet channels are going to be more widely used, the need for trust and confidence presents many demanding technical challenges, including authentication, non-repudiation, data integrity.
  - To support high availability of information flow and requirements on the frequency of the loss of flow and on the duration of the loss of flow.

It is important to note that the same system can have different dependability requirements depending on the stakeholder perspective.

3.2 Threats and vulnerabilities

In a risk based approach to dependability requirements elicitation, the notions of threat and vulnerability are important. A threat is understood as an event that potentially causes a loss. A threat can be of accidental or malicious nature. Different loss categories were described in the previous section. In the special case of a threat causing a safety loss, it is refered to as a safety hazard. Finally, risk is generally understood as the combination of threat occurrence and severity of the associated losses (Risk is the product of (threat * loss)).

A system vulnerability is understood as a weakness or flaw in the underlying system that can be exploited for inducing threats. Generally vulnerabilities are of technological or organisational nature. In [3], H. Anderson, has defined 20 categories of technological vulnerability attributes which an essential information infrastructure should address. The study focused on systems in the defence area but the majority of vulnerability categories are applicable in the health domain. Some of the relevant categories include: inherent Design/Architecture weaknesses, complexity, operation near to capacity limits, dependencies between systems.



System dependability requirements are derived from stakeholder requirements. Ideally, when formulating system requirements, threats should be taken into account. Indeed, proper knowledge of realistic threats allow a system designer and operator to include the necessary design mechanisms and protective measures to counteract the threats. Some threats can be foreseen, their likelihood assessed, and taken into account into the system design. This is part of current best practice in dependability engineering. However, for large-scale interdependent systems-of-systems, there are problems in predicting threats because of:

- The lack of complete knowledge of the end-to-end system and its interactions;
- The dynamically changing user environments due to system evolution and mobile applications;
- Complex failure semantics caused by subtle interactions between the environment, technological system and the human operators.

In this case, there is a need to provide defensive measures to guarantee critical requirements. A whole new research area in the field of *Survivability* addresses this problem [4]. The term survivability denotes "the ability of a system to continue the adequate performance of its critical tasks even in the presence of unforeseen attacks, failures and accidents". We concluded in [5] that a definition of survivability as another system attribute aligned to security, availability, reliability and safety was not justified. Indeed survivability, is useful as

an emergent system *property*, but can still be expressed by means of the above dependability *attributes*.

Below, we will illustrate some categories of risks pertaining to privacy, safety, service insecurity and unavailability from the perspectives of threats and vulnerabilities specific to the health sector.

3.2.1 Privacy

The health sector has a long tradition of protecting patients' privacy and for confidentiality in the provider-patient relationship. It is an integral part of medical practice. However, many of the proposals for reforming the practices of the health system through the use of IT have serious implications for the privacy of patient records. Strong arguments have been cited [5] to suggest that the deployment of technology is advancing without sufficient forethought to, or the implementation of, privacy protection policies. There are three major issues for concern:

- Electronic health records contain personally identifiable data and are susceptible to fraudulent abuse and to abuse of privacy and personal integrity. Even when mechanisms are in place for anonymising data e.g. by means of key codification, data are still potentially traceable to their origin by means of powerful computing systems and search mechanisms in databases.
- Health records are used in many distributed health systems. The perception of the benefits/risks related to the use of new health care systems and the awareness of security problems are diverse throughout Regions. E.g. Finland experiences a high Internet penetration and advanced protection systems are in place (e.g. strong encryption smart cards). On the other hand, the majority of systems being proposed predominantly rely on simple protection mechanisms (e.g. firewall technology) to implement security policy and protect against intrusions.
- IT security policies need to be adapted to cope with the changing health care context. Whereas, in general, the Health sector has high ethical standards and procedures for processing health records, it often lacks the necessary internal technical expertise to implement and maintain secure IT systems.

We will deal with some threats to privacy in turn.

a.-) Privacy invasion by commercial exploitation of data

With the move to centralised electronic records there is now the potential for health information to be exploited on a large scale. For example, quoting from Anderson [6], it is reported that a large US pharmaceutical company gained access to a prescription database covering over 0.5 million prescription users. They are said to be mining the database in search of patients whose prescription requirements fit depression related illnesses, with a view to promoting the use of one their drugs by contacting the patient's GP's. It is also reported that many health insurance companies (as high as 40%) pass on medical information to third parties, such as financial institutes or employers, without the permission of patients. Employers, for recruiting, routinely use this information and other personnel related issues. These detrimental practices could be severely exacerbated by the centralisation of digital health records.

b.-) Intrusions and internal abuse

Central to a distributed health care system is the concept of a regional or national database for health records. Hospitals will be connected to this system via a secure local intranet, and

to each other via the same intranet. Pivotal to the concept of electronic health records is the integration of local General Practitioners, and the electronic transfer of GP records to the central servers. It is envisaged that GPs will be linked to the health service systems via the Internet. The use of a dedicated intranet on a national scale would be unfeasible due to the cost of implementation. To provide security between the Internet and the health systems intranet and file systems firewalls are installed. The purpose of the firewalls is to prevent information flow out of the health systems and to control input to the systems. However, there are numerous dependability flaws inherent in this approach, when applied to unbounded network infrastructures such as the Internet.

1. Firewall technology is not yet proven, and there are doubts over the level of security provided by these mechanisms. For example, using eavesdropping it is possible to determine system passwords to penetrate firewalls. Although in such circumstances firewalls may prevent information being extracted from the host system, they do not prevent data being corrupted or modified within the system. Instances of medical records being tampered with via remote Internet accesses have already occurred [6].

2. A firewall security approach does not provide security of data in transit, between remote user and host system. Clearly, in the scenario envisaged, where medical records will be routinely transferred between a centralised host server and remote GP there is an essential requirement to ensure the confidentiality and integrity of data that is transmitted.

3. Firewall technology does not necessarily provide protection from abuse by users *internal* to the host system. Centralised electronic health records will mean that there is a significantly larger number of individuals that have access to an individual's medical information (potentially in the thousands, rather than the tens of people typically associated with paper based records). The removal of informal security mechanisms implicit in the nature of localised paper based records leads to the far greater possibility of malicious or accidental abuse by employers within the health sector. In a recent analysis of issues pertaining to patient confidentiality in networked UK national health systems Anderson [6] quotes the following example of health information abuse that occurred in the US, by an executive who had access to health records:

- A US banker, on a state health commission, was able to gain access to a list of all the patients diagnosed with cancer in the region. He was able to cross-reference this list with clients of his bank and call in the loans of the affected patients. [7]

c.-) Flaws in health organisations' security policy

Dependability, and especially the security facet, relies on an institute defining and exploiting a well thought out and well implemented security policy [8]. Implementing and maintaining this policy typically requires the services of full time systems security personnel. There are many justifications for this:

- Implementing dependable systems is a complex and difficult task requiring a broad appreciation of systems and dependability issues. Non-specialists rarely have the requisite experience or knowledge;
- Although off-the-shelf packages are available for implementing security policies, it is typical that information systems security relies upon the use of a number of diverse approaches and applications. These implementations make use of low-level systems features and require firm understanding of operating systems issues and idiosyncrasies. Again, non-specialists rarely have the appropriate depth of knowledge;
- Security and dependability policies are not static entities. Threats, risks, environments and operating systems are in a highly dynamic state of change in the IT world.

Consequently, the security policy implementation must adapt and advance in line with (or even ahead of) other hardware and software systems issues.

Despite these risks, it is typically the case that many health organisations do not employ the necessary trained, professional security staff. The reasons for this are largely economic. In a climate where organisations are dealing with budget cutbacks and 'down-sizing' (particularly true in the health sector) it is difficult for managers to accept the economic benefit of IT security staff. Dependability and security clearly are not yet perceived as contributing factors to productivity, nor are they currently perceived as high priorities in many businesses. It may well need legislation (or lawsuits) before the necessary investments are made to ensure high security high dependability IT systems in the health sector.

3.2.2 Safety

Patient safety remains the most important concern in health care. Related to safety risks in an information intensive healthcare system, information integrity and availability of information flow are becoming critical requirements. For whatever reason, it must be accepted that errors may occur in the health care information systems both with respect to patients' medical records and to clinical advice affecting either diagnosis or treatment. If incorrect information is provided then inappropriate treatment may result in extra patient suffering. A serious incident that happened in January 1999 in a European Hospital [14] illustrates the criticality of information. The incident was caused by wrong drug information as provided by the pharmaceutical company. The resulting incorrect treatment with the drug caused the death of several patients. Patient safety directly depends upon verification processes at the sharp end of the system, where transformations occur involving the patient and/or related objects. These objects can be pure information objects (e.g. records, lab results, prescriptions, drug information), physical objects obtained from the patient (e.g. blood samples, tissue for histopathology) and objects intended to be used for a specific patient (e.g. medications, prosthesis, transplants).

3.2.3 Secure infrastructure services

There are several issues that need to be fully addressed:

- Confidentiality of transmissions so that information cannot be stolen by eavesdropping;
- Data Integrity so that data cannot be modified on route or during storage;
- Assuring identity of stakeholders and health workers including authentication so that all involved parties are confident that the communicating individuals in the exchange are in fact who they purport to be and non-repudiation so that no individual can deny involvement in a transaction or deny responsibility in a task execution.

If each of the above issues is not fully addressed then there is scope for considerable abuse in health information systems. Some simple examples will illustrate this. In the UK the case of a sex stalker has been reported. The individual, who had access to health records, was able to contact women and discuss their family medical history with them. With this detailed information it was possible for him to try and convince young women to arrange an appointment to see him [6]. This extreme example of medical information abuse demonstrates how important it is to be able to authenticate the individuals in an Internet service. However, less extreme but equally as important issues can be readily identified. If medical records are to be transferred between GP's and a centralised medical information system, it is imperative that the individual that is submitting the records can be authenticated. This has safety and confidentiality implications, as well as legal. Similarly, it is essential that individuals are not only correctly identified but also that they cannot refute responsibility for

a communication pertaining to an individual's health care. For example, it should not be possible for a consultant or doctor to refute responsibility for a diagnosis that had led to inappropriate patient treatment.

3.2.4 High availability of health care processes and services

There are increasing dependability constraints within advanced or future health systems that will demand high *availability* of services and communications. The most obvious demands are presented in the area of remote health care. For example, it is expected to become increasingly possible to provide 24hr remote and automated patient observation, using microelectronics and home computer technology. This has been possible with traditional technologies and using dedicated telephone lines, however, there is the potential for remote health monitoring and diagnostic systems to become far more wide scale through the use of the Internet. The majority of remote health care systems are unlikely to be critically dependent upon guaranteed Internet access, however, in some cases there could be a strong requirement for predictable and reliable internet communication (systems for dialysis or heart monitoring are obvious examples). High guaranteed levels of availability may also be required for remote collaboration facilities, particularly in the circumstances when these services might be used for operations performed under remote supervision.

Another systems scenario that will demand high availability is the infrastructure linking health sectors and government services, particularly those in connection to emergency services (for example, for disaster contingency management). In the strategic information warfare study [8], conducted in the US, it was shown that current Internet technology can be easily (and remotely) attacked such that messages and communication channels can be blocked. In the event of a military or terrorist attack, it would be possible, under current systems scenarios, for the hostile party to compound the effects of an attack (for example, a terrorist bombing) by intercepting and blocking Internet communications between the Government, emergency and medical services.

4 Case Study: The integrated drug delivery environment

4.1 Introduction

The case study provided by the Health Care Enterprise (HCE) is the Pilot Integrated Pharmaceutical Environment. The objective of this project is to integrate all the drug delivery processes of the HCE with the logistics processes in the drug supply chain. An important challenge with this approach will be to properly control in real-time the flow of information at the point of use (patient). Some information (e.g. drug characteristics) is derived from the supply chain whilst other information (e.g. drug needs) could also be feed into the supply chain. The potential benefits of such an integrated approach are twofold:

- Clinical: Avoidance of preventable errors in the drug therapy process and as such improvement of patient safety. Adverse Drug Events (ADEs – i.e. clinical adverse events suffered by patients as a result of non appropriate drug therapy process management) are one of the major classes (20%) of adverse events revealed in a Medical Practice Study performed by the Harvard School of Public Health [9]. In particular, for one large hospital a summary of results are: 2.43 drug errors occurred every 100 hospitalised Patients; Patient experiencing an ADE had 1.88 increased risk of death, i.e. mortality almost doubled. Each error prolonged patient stay of 1.91 days and the increased associated costs were $2262. The error distribution reported for drug therapy process is:
    - 49% errors occurred in the ordering stage
    - 26% errors occurred in the administration stage

- 14% errors occurred in the dispensing stage
- 11% errors occurred in the transcription stage

- Economical: It is expected to save as much as 50% on logistics costs in the HCE/pharmaceutical companies/distributors chain.

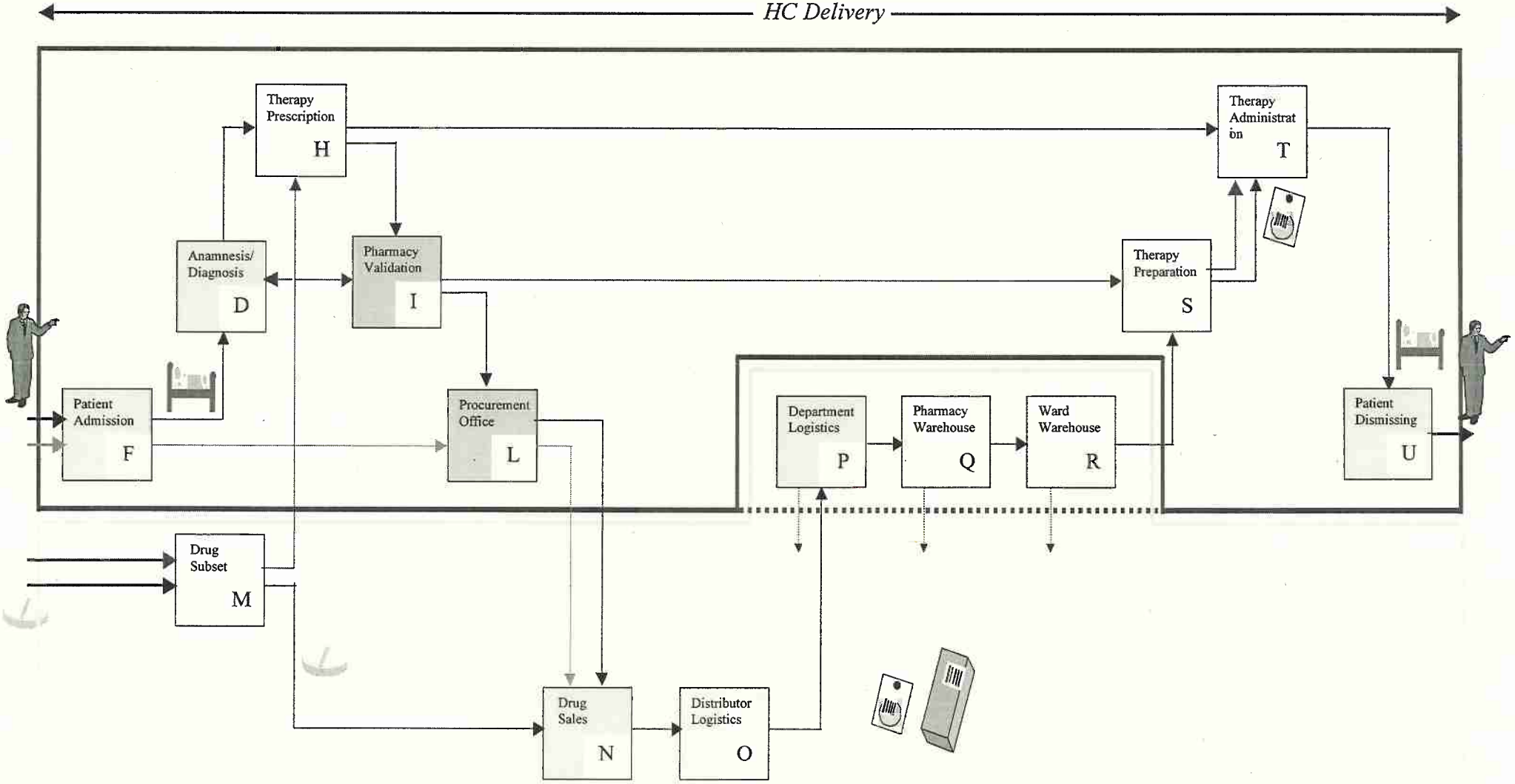
4.2 Business processes in the integrated drug delivery environment

Let us consider the drug delivery process for a hospitalized patient. It is hierarchically composed of other sub-processes, including diagnosis, therapy prescription, drug preparation and therapy administration. Each of these sub-processes is composed of specific tasks that range from complex decision making (patient diagnosis, therapy prescription) to routine and repetitive ones (dose preparation, therapy administration). Either type of task depends on a series of administrative controls intended to assure coherence with clinical rules and regulatory controls to assure coherence with patient safety norms.

The following figure 3 gives an overview of the different tasks involved in the drug delivery process. Refer to [10] for a detailed process, task and information flow analysis of the drug delivery process. Tasks are classified under 4 categories:

- Clinical tasks, requiring critical know-how and considered as part of core business processes of a hospital and involving medical knowledge and experience. This is the case of drug administration.
- Clinical support tasks, representing the hospital general background, and not involving specific knowledge. In this scenario, a clinical support task is represented by therapy preparation: an operator (not necessary a nurse) is in charge of collecting the necessary doses assigned to each patient in the personalised therapy before the administration.
- Non-clinical tasks, considered as activities not directly linked to core businesses but essential as basic mechanisms for the functioning of the overall system. This is the case of patient admission or data management, for instance.
- Product or service supplier tasks (e.g. drug supplier), considered external to the hospital but participating in the functioning of the health care system or virtual hospital.

Figure 3: DRUG DELIVERY PROCESS



4.3 Generalised information flow model

In the previous section, health care processes involved in a drug therapy were described. Based on that description, a generalised information flow model is deduced. As we focus in this case study on the information dependability aspects both from the information product (content) and the information flow points of view, the model will help us in defining a dependability requirements elicitation process. The information flow model proposed in figure 4 is representative of the health care sector and covers the end-to-end support from source to point of delivery of the information. The model includes:

- Health care tasks performed on patient related physical or data objects. Examples of physical and data objects are given below. Information flow does not itself produce healthcare value. At the point of care, healthcare value is, in fact, produced when the information flow interacts (directly or indirectly) with the patient related object by means of health care process tasks. These tasks are executed by human operators, by medical devices or by a combination of both.

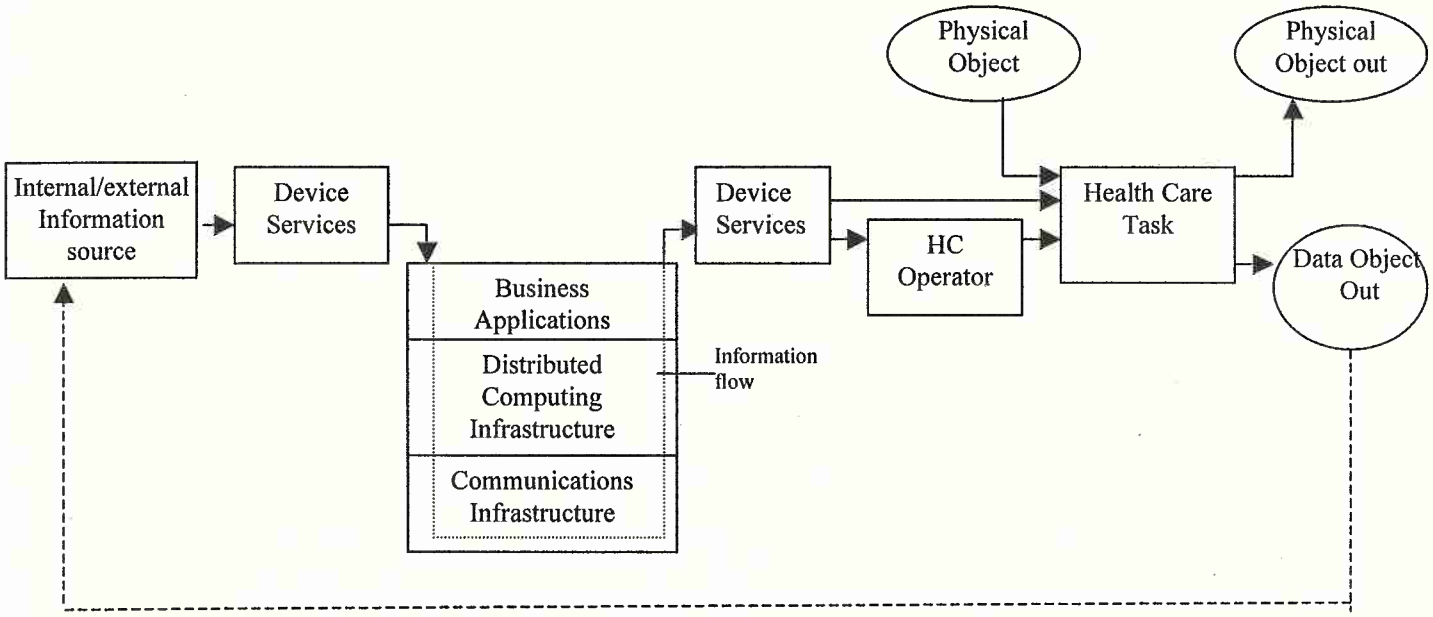


Figure 4: Simplified Information flow model

- Health Care operator: Primary information consumers are the healthcare operators (Nurses, Doctors, Laboratory analysts, etc). They interact with the patient in the process by performing process specific tasks, as defined in specific organisational rules and procedures. Process specific tasks range, within the specific profession domain, from complex decision making to simple routine and repetitive tasks.
- Services provided by devices that participate in the information flow. These range from computer interfaces to automatic data capture devices (e.g. optical reading), to devices for personal identification (e.g. smart cards). In addition, medical devices provide information to a human operator (e.g. diagnosis) or interact directly in the tasks in an automated way (e.g. therapy administration).

- Business applications supporting the health care processes (e.g. pharmacy, laboratory).
- Information Infrastructure consisting of:
  - Distributed computing infrastructure as the system that stores, processes and supports retrieval of the information.
  - Communications infrastructures (e.g the Internet) as the system that supports the transmission of the information.
- Information source creates or collects information. The information originates from within the health enterprise as well as from outside suppliers.

Two main types of patient related objects are involved in these interactions. They include physical objects and data objects:

- Physical objects of patients, including the patient himself. Examples include:
  - Patient-output related objects (biological samples, organs, etc.) for in vitro activities deriving from service contracts (laboratory medicine, pathology, etc.)
  - Patient-input related objects bound to in-vivo activities on Patients (drugs and medications, transplant organs, transfusions included, medical devices, etc.)
- Data objects that directly represent patient attributes. They could also represent information necessary for performing the tasks on patient objects and include:
  - Patient identifiers.
  - Service contracts about patients (e.g., diagnosis/therapy prescriptions, entitlement/billing, etc., both in an inter- or intra-enterprise context),
  - Information necessary for performing in vivo activities directly on patients (diagnostic imaging, phlebotomy, drug therpay, etc.). For instance drug related information for drug administration.
  - Patient healthcare reports that are the output of service contracts (e.g. X-rays, lab test results, etc.).
  - Patient healthcare records (integration of Patient healthcare reports on a historical basis).

An example of data objects applied to drug administration is given in figure 5.

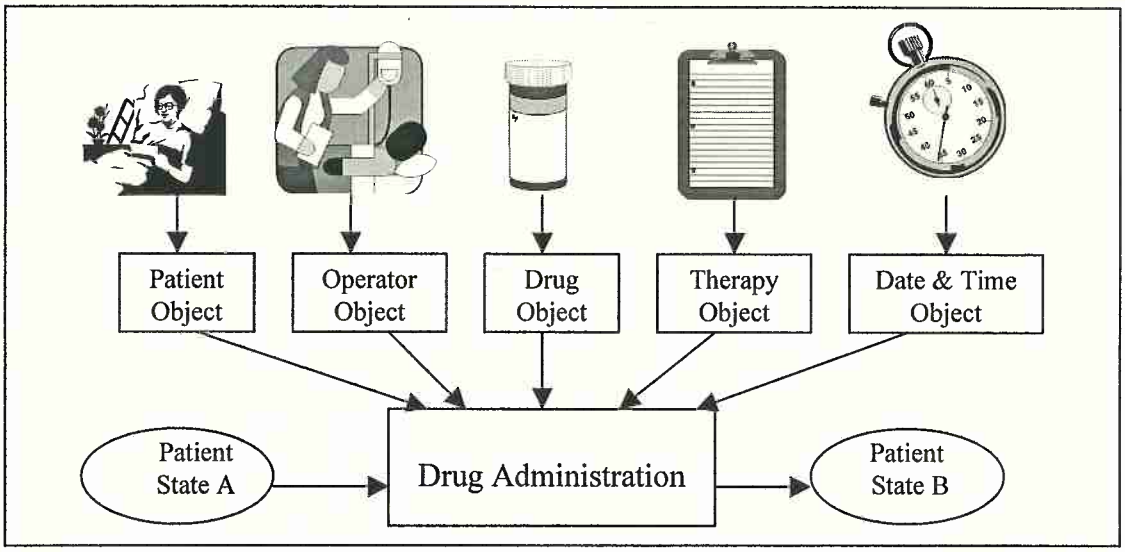


Figure 5: Types of data objects: example of drug administration

The data objects depicted in figure 5, each contain a set of data items necessary for performing a specific health care task (e.g. drug administration). Dependability requirements can be associated with these data items (figure 6). These requirements are derived from the nature of the data item and from the risks involved in executing the task in which the data item is used. For instance, for a critical task such as drug administration, the authentication of the patient is crucial.

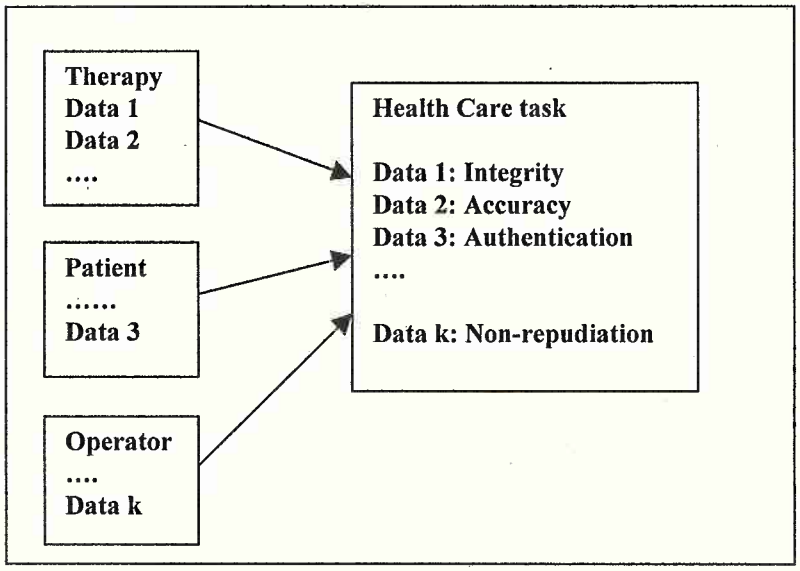


Figure 6: Data items requirements

4.4 The generalised set of dependability attributes

In this section, we propose a generalised set of dependability attributes that serve at defining application-specific user dependability requirements in the health care sector.

We have previously underlined the information intensive nature of health care processes and have provided a generalised information model in the previous section. Based on that model, we propose **data object, information flow** and **stakeholder identity** as three major categories of user requirements. As a fourth category, we propose **functional safety**. These four categories will populate the generalised set of dependability attributes applicable to critical health care tasks.

1. Data object attributes characterise the *information content* of data. In this respect, results from the information quality research area are of relevance here. According to Wang [11], Information Quality (IQ) is " fitness for use by information consumers" and is characterised by a set of attributes classified under four broad IQ categories. Of importance to our work are three attributes that include: Accuracy (Intrinsic IQ category), Security (Accessibility IQ category), Timeliness (Contextual IQ category). We have further subdivided the security attribute into the integrity, confidentiality and authenticity attributes.

Data object attributes	
Integrity	Remaining in an unimpaired condition
Accuracy	Representing the current real-world state
Timeliness	Accessibility when needed
Confidentiality	Disclosure to authorised persons only
Authenticity	Guaranteeing the authorship and/or ownership of the information product

2. The stakeholders involved in health care provision were identified in section 3.1. Important stakeholders at the point of care include the patient and the health care operator. *Stakeholder identity* requirements characterise the identity of health care workers and patients in data transactions and during the execution of health care tasks.

The authentication attribute in the stakeholder domain differs from authenticity attribute in the data object domain in the following aspect. Authentication focuses on the transaction instead of the information content. This means that the source of the information transfer is authenticated (computer, sender) but not the information itself. This distinction is necessary because there could still be a gap in the trust chain between the author's intentions (code, information) and the code/information itself.

Stakeholder identity attributes	
Authentication during transaction	person who claims to have sent the message is in fact the person who sent the message
Non-repudiation during transaction	sender of the message can not deny having sent it
Authentication during task execution	determination that presumed identity of patient and worker are valid during task execution
Non-repudiation during task execution	worker cannot refute responsibility for an action during task execution

3. Dependability attributes of information flow services characterise requirements on services provided by devices that participate in the information flow or on services for end-to-end transmission. In the telecommunications services sector, considerable research work is being performed in the field of characterisation of "Quality of Service" (QoS). It focuses on end-to-end service quality, that is, the complete media flow from application-to-application rather than just on the aspects of the network system's internals. The QoS related attributes that are useful to our work include performance and level of service [12].

Information flow attributes	
Reliability	continuity of information flow
Availability	readiness for usage of information flow
End-to-end trust	assurance of a trusted flow path between end systems
Performance	throughput, delay, jitter, loss rates
Level of service	deterministic, predictive (probability bounds), best effort

4. Functional safety is particularly important in cases in which there exists a direct interaction of a medical device with a patient in a (semi-) automated way (e.g. radio-therapy machine).

Functional safety attribute	
Safety	Avoidance of safety-related events

4.5 A requirements elicitation process

A process for eliciting application specific dependability requirements is outlined in figure 7.

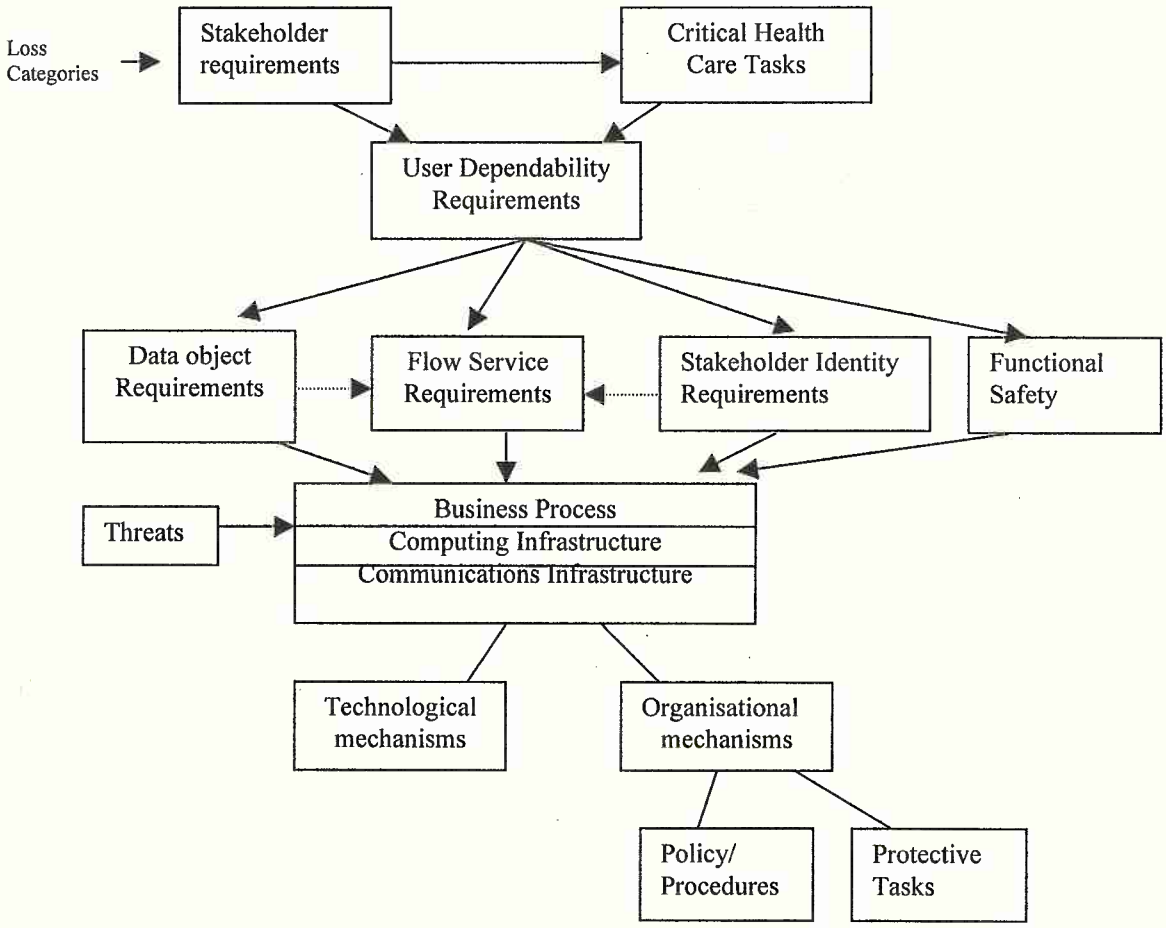


Figure 7: Requirements process

The elicitation process starts from knowledge about specific stakeholder requirements and about involved critical health care tasks. A task is considered critical when its malfunction creates a risk. For instance from the patient safety perspective an adverse drug event in drug administration creates a safety risk.

The set of dependability attributes described in the previous section, contains four categories of attributes that have to be instantiated into user dependability requirements for the task at hand. Afterwards, an important challenge is to map the heterogeneous set of user requirements to a system requirements specification.

We have taken business processes, computing infrastructures and communications infrastructures as the three major layers of systems for which dependability requirements need to be specified in order to achieve the user dependability requirements. System requirements are applicable to any or all layers.

In [13], Laprie et al. provide four types of dependability mechanisms for satisfying system dependability requirements: Fault Tolerance, Fault Prevention, Fault Removal and Fault Forecasting. These are classes of methods and techniques that allow 1) to provide the ability

to deliver a service on which reliance can be placed and 2) to reach confidence in this ability. An additional dimension is to distinguish between technological mechanisms and organisational mechanisms both applicable during design and operation of the system. The organisational mechanisms at the business process layer are particularly important for applications of large-scale infrastructures and services such as health care for reasons explained under section 3.2. For instance, in health care, contingency plans or specific control tasks can be applied to cope with adverse events. These tasks can be supported by technological mechanisms. For instance, the use of automatic data capture devices (optical, magnetic, smart cards, etc) offer the possibility to create "labels" of portable information for automatic processing, thus enhancing the potential for safer and more efficient controls in health care processes.

One positive point is that some of the mechanisms required for addressing dependability requirements in health care, such as authentication, non-repudiation and confidentiality during message transactions, are generic to transaction management in the e-commerce domain. This overlap means that medical systems may benefit from the substantial private funding being invested in Internet commerce. This is the motivation of the PCASSO project [15] , sponsored by the US National Library of Medicine, which tries to apply state-of-the-art security technology to tele-medicine applications over the Internet. It should be noted that electronic commerce solutions such as Netscape's Secure Sockets Layer (SSL) and Visa/MasterCard's Secure Electronic Transactions (SET) were designed to solve the problem of securing transactions between a Web browser and a server. These solutions also have applicability in healthcare transactions. However, an important challenge is to transfer these solutions to the health care sector consistent with sector specific requirements in order to dependably support the use of patient medical information at the point of care. These requirements imply:

- The capability to assure the dependability of the data content;
- The capability to protect different levels of sensitivity of data;
- The capability to protect data in the client environment;
- The capability to enable by-passing of the security controls in emergency situations.

5 Conclusions

By means of an example from the drug therapy and the drug supply chain, we have demonstrated in this report that health care processes are highly dependent on information and knowledge management. Thus the collection, provision and processing of timely and correct information by means of advanced information infrastructures is determinant from a patient safety perspective.

Moreover, the advantages generated by business integration by means of information infrastructures are also apparent: health care enterprises benefit from information sharing within the alliances established with suppliers, by means of enhancement of knowledge, capability and service management.

Paradoxically, this higher dependence on information flow for enhancing patient safety and service quality, also introduces new threats and risks. In this case study, we have taken a harmonised approach, that starting from a number of realistic threats and business scenarios, characterises dependability requirements from the perspectives of the various stakeholders involved. Major challenges still exist for translating these heterogeneous requirements to suitable system architectures. Fortunately, there are techniques from the e-commerce domain that can be transferred to the health domain for instance for enhancing trust in information transactions on open infrastructures. But additional stringent user requirements specifically

related to privacy and data integrity require architectural approaches for dependable storage and retrieval of information products during the execution of health care tasks. These approaches need to be smoothly integrated with the transaction part of the processes.

6 Acknowledgements

The authors would like to thank both Jari Forsstrom for reviewing this report and for his valuable comments.

Jari Forsström
Medical Informatics Centre Turku (MIRCIT)
Kiinamyllynkatu 4-8
20520 Turku, FINLAND
Tel: +358-2-2612914
GSM +358-40-544 1809
Fax: +358-2-2613920
forsstrom@multimedica.com
URL: http://www.utu.fi/research/mircit

7 References

1. M Prigg; Robots try their hand at Surgery, Sunday Times, 15th February 1998.
2. EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Official Journal L 281, 23/11/1995.
3. Robert H. Anderson, RAND. A "Minimum Essential Information Infrastructure" (MEII) for US Defense systems: Meaningful? Feasible? Useful? In proceeding of the second Information Survivability Workshop. Orlando, USA, 28-30 October 1998. IEEE Computer press.
4. T Jackson, M. Wilikens, Survivability of Networked Information Systems and Infrastructures. State-of-the-art study. JRC Technical report I.98.70, February 1998.
5. Ross Anderson, Patient Confidentiality - At Risk from NHS Wide Networking, Proceedings of Health Care 1996 (http://www.cl.cam.ac.uk/users/rja14/hcs96.ps.Z).
6. Anonymous, RMs need to safeguard computerised patient records to protect hospitals, Hospital Risk management 1993; 9 (Sept), pp129-40.
7. John Austin, Co-ordinating an Investigation, Computer Security Incident Handling Workshop, Missouri, Aug 1993.
8. Roger C. Molander, Andrew S. Riddle, Peter A. Wilson. Strategic Information Warfare, National Defence Research Institute (U.S.), RAND 1996.
9. Leape L. Error in medicine. Journal of American Medical Association (JAMA), 1994: pages 1851-1857
10. C.Bracuti, A.Sanna: Health care virtual enterprise: Process, task and information flow analysis. Joint Research Centre Technical Report I.99.53, March 1999.
11. Richard Y. Wang. A product perspective on Total Data Quality Management.. Communications of the ACM. February 1998, vol 41, no 2.
12. Aurrecoechea, C., Campbell, A.T. and L. Hauw, "A Survey of QoS Architectures", ACM/Springer Verlag Multimedia Systems Journal , Special Issue on QoS Architecture, Vol. 6 No. 3, May 1998.

13. Dependability: Basic Concepts and Terminology, A. Avizienis, H. Kopetz, J.C. Laprie (eds.), Springer –Verlag, 1993.

14. Twee baby's sterven na toediening verkeerd medicijn (Two babies die after wrong drug administration). De Standaard/Het Nieuwsblad, 18th January 1999.

15. B.Baker et all. PCASSO: Applying and Extending State-of-the-Art security in the healthcare domain. 1997, annual computer security applications conference.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

EUROPEAN COMMISSION
JOINT RESEARCH CENTRE