"Co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union"

Report No: WP3 / D3.1

Generic hospital model (as is) from task 1. i.e. a reference model of an unprotected hospital including : processes, activities, actors, resources and evaluation indicators

Version: 0.6

Date: 23 Sept 2015

Authors: DB, RF, SV (OSR) AG, JF (INSA Lyon)

Approved by: CA

Contents

Executive Summary

The potential for a terrorist attack against a hospital within the European Union (EU) has not been a routine question addressed by hospital security and business resilience managers, but the current trend in terrorism in the West provides ample evidence that an attack against a hospital cannot be ignored. The impact of such an attack and the direct and indirect consequences to the hospital, including disruption to critical assets, will be addressed in this paper. The research team will identify the most critical assets or functions of the hospital in order to create a simulation model whereby a series of terrorist scenarios can be simulated and the effect to each asset can be observed as an 'as is' model of the hospital that will potentially reveal any areas of vulnerability or gaps that may exist. Future work package three (WP3) activity will include the identification of any necessary enhancements to the hospital emergency management plans by conducting the self-assessment audit process that will be included in D1.6 and form part of the THREATS toolbox of measures.

This report has been informed by previous THREATS work that was carried out by work package one (WP1) and work package two (WP2). The collective THREATS research provides useful context and insight to the poor availability of guidance throughout the EU Health Sector for the preparedness and contingency planning for a direct terrorist attack of a hospital (see D2.1), something that is in stark contrast to the preparedness of international transport hubs such as airports, railway hubs and docks (see D1.3 and 1.4). The literature lacks evidence that terrorist threats have been used to inform modelling of risk scenarios, to enable emergency management systems to be assessed for their reliability and usefulness when managing the consequences following an attack. The legal framework and common practices to enable the management of interdependent European Critical Infrastructure (ECI) vary across EU Member State (MS) and the level of critical infrastructure protection (CIP) is inconsistent (see D1.1).

Terrorist attack methodology has been briefly analysed to inform the terrorist scenario design process. Although terrorist modus operandi (MO) can change, the current themes identified in D1.3 have been used as a baseline. A security and vulnerability assessment (SVA) methodology has been adopted to identify the most vulnerable assets and functions of the hospital. The terrorist MO has then been combined with an asset/function vulnerability to produce a risk matrix that will be used to develop a simulation model.

The IDEFØ/CPLEX simulation method has been adopted for the simulation modelling that will support the research of WP3. A large hospital in Milan, Ospedale San Raffaele (OSR), has been selected to test all theories, simulations and practical application of measures because the hospital represents a typical large hospital with a broad scope of general and specialist medical activity, including medical scientific research activity, and serves a large population group. Moreover the hospital is considered to be part of the critical national infrastructure (CNI).

1. Introduction

1.1 Ospedale San Raffaele

Ospedale San Raffaele (OSR) is a large health complex that is made up of a general hospital that provides general medical services and almost all of the specialist medical disciplines are provided. OSR has over 1,300 beds and according to OSR admissions data for 2014 the hospital treated 895,000 out-patients, 63,500 observations in the Emergency Department and almost 50,000 in-patient admissions with 35,000 surgical procedures being performed. The staff at OSR total nearly 6,000 employees with 660 scientists, researchers and 1,000 students and volunteers as for the “Chart of Services”. The OSR health complex is significant and a disruption to the services it provides is likely to have an impact across multiple areas of CNI.

1.2 OSR Critical Assets

Due to the size of OSR the research team anticipated the quantity of critical assets or functions at OSR to be numerous and so it was decided at an early stage of the research that a sample of critical assets or functions would be selected for this work. The selection criteria would be constrained to the areas of criticality that were most vulnerable to a terrorist attack, these areas may include assets or functions that are easily accessible or don’t have particularly robust protective measures or resilience contingencies in place. It was a challenge to quickly identify suitable areas of criticality because at first glance many things appear to be critical to the function of the hospital but the team agreed with the North American Electric Reliability Corporation definition that ‘critical assets are facilities, systems, functions, or equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability and operability of the system’ [Bulk Electric System]’ (NERC, 2009:1), this definition would provide the baseline for the selection of assets or functions that would potentially be critical. Once assets and functions had been defined critical they would be risk assessed against their exposure or vulnerability to terrorist threats.

1.3 Risk Assessment

Work conducted as part of D1.1 and D1.2 was used to inform the risk assessment process by providing useful data relating to terrorist MO. The type of terrorist methodology was used to help identify potential forms of attack and where a potential terrorist attack may present the highest likelihood of mission success in terms of collateral damage, loss of life and disruption to business. A substantial committee was formed with representatives of the clinical and research departments; security department, maintenance department and the prevention and

protection department and they were challenged to identify their departmental areas of criticality, vulnerability and discuss the simplest way to damage or disrupt the asset or function. The result of the process was to create a risk matrix and correlate some of the risks/vulnerabilities to potential forms of terrorist attack. The THREATS critical pillars of physical protection of buildings and assets; security of people and protection of data and information (see D1.2) was used to group each of the vulnerabilities and reduce duplication of effort because a single effect could potentially have cross over to other vulnerabilities and the THREATS team are keen to utilise common themes and language that can be used in any hospital throughout the EU. It is worthy of note that such a kind of committee is not formalized as a "Business Continuity or Security Committee" in OSR and it was formed specifically because of the THREATS project. In fact a business continuity management (BCM) or security plan does not exist within OSR.

1.4 Vulnerabilities

A common theme emerged from the risk assessment process that many of the vulnerabilities related to the 'open public access' of the hospital and anyone from the general population could enter the hospital complex at any time of the day or night and gain access to the hospital facility without having to negotiate any security screening measures. The openness of the hospital is due to the hospital's mission to welcome and receive people in need but this principle presents a vulnerability that has cross over to all departments at OSR. Therefore the modelling effort was focused upon the flow of pedestrian traffic throughout the complex, with the aim of identifying the way people enter and leave OSR, how they move from department to department and where the main concentration of people are within OSR and at what time of day are the main migrations of pedestrian traffic. This data would be useful to identify key areas of vulnerability within the public areas and may help to understand when and how a terrorist could strike at OSR.

Other vulnerabilities recognized by the committee are:

- The presence itself of hazards inside the hospital (like nuclear and biological material, for example) and the relatively scarce security protection of them that increase extremely their attractiveness to terrorists
- The dependence of almost all the hospital processes on the informatics that can represent an important weakness on business continuity in case of malfunction/disruption
- The level of dependence of a lot of the people (patients) steadily present inside the hospital: it represents an important vulnerability in case of need to evacuate all or part of the hospital.

1.5 IDEFØ Model Methodology

The IDEFØ model methodology was selected to provide a visual illustration of the migration and flow of pedestrian traffic throughout OSR. The IDEFØ method is useful because:

- It enables a hierarchical approach of a wide system such as OSR, using a black-box decomposition that enables the possibility to detail or not a part of the system (e.g. a care unit or a technical unit).
- It can be used to decompose a system with a physical view or a functional view, specifying respectively the hospital map and the care unit processes, in both cases with the same language.
- It proposes a very simple language based on two elements (boxes and arrows) that is very close to the mental representation of actors (places and paths, or activities and their successor links).
- It is also a very good communication tool which allows drawing instead of writing or speaking.

The map of the hospital and the process structure of care units can be easily translated to an access matrix that can be used to define the core structure of a dynamic model. Moreover, the IDEFØ method has already been successfully applied, by a member of the research team, to the modelling of a French hospital, Centre Hospitalier St-Joseph/St-Luc, Lyon. The OSR hospital map has been modelled with a physical approach and later the Emergency Department with a functional approach.

The results of the modelling process, modelling of an unprotected 'as-is' hospital, and risk assessment of terrorist threats will enable:

- The creation of a reference model of a hospital that is part of the CNI, which can be analysed and used for future simulations of terrorist scenarios in the hospital environment.
- The creation of a hospital risk matrix directly relating to terrorist threats which can be used to test some terrorist scenarios in the hospital setting.
- An understanding of the model limitations and its strengths when used to simulate terrorist attacks in the hospital setting.
- A better understanding of the potential impacts of a variety of terrorist attacks against an unprotected hospital.
- The potential to identify and understand the type and level of security measures and the BCM required to improve the resilience of a hospital to terrorist attacks.

- To propose a ‘to-be’ model of a better prepared hospital.

1.6 Scope

The purpose of this report is to analyse the hospital business process and by doing so, illustrate the multiple operational activities that take place at the hospital routinely. This research may provide a deeper understanding of the way a hospital functions at every level and provide an indication of the critical activities, processes or functions so resource and effort can be applied appropriately to restore the activity to an acceptable level following a disruption due to terrorist attack. Furthermore the report may provide an indication of the simple but layered security measures and BCM activity that could help to mitigate the impact from an attack.

The modelling approach has been adopted because of the potential value that could be added to understanding the way a hospital functions under the current circumstances and will be presented in this report as the ‘as is’ model. Future THREATS activity will apply the toolbox of measures that are currently being developed as part of D1.6 and applied to OSR so the simulation can be run once more and a gap analysis conducted to evaluate the effectiveness and validity of the toolbox of measures.

2. Design and Analysis of terrorist attack scenarios

2.1 The Threat

Although terrorist organisations and lone actors have not deliberately targeted hospitals in the West, except for historical attacks such as the attack at Musgrave Park Hospital in Belfast by the Irish Republican Army in 1991 (Ganor and Wernli, 2013:28), hospitals have been deliberately attacked in other parts of the world. Many of the 100 terrorist attacks of hospitals listed by Ganor and Halperin-Wernli (2013) took place in countries that were gripped by civil war and the hospitals may have been attacked by formed military organisations, as opposed to terrorist groups or individuals. However recent terrorist attacks throughout the EU demonstrates that terrorism knows no boundary and therefore any attack that will produce an impact may be considered 'fair game'. D1.3 illustrates the porosity of current security measures at hospitals across the EU, the limitations of security measures can be highlighted by the level of crime, in particular the loss of pharmaceuticals and equipment (see D1.5).

2.2 Security Vulnerability Assessment (SVA)

The SVA methodology helps managers to identify, analyse and manage the physical security vulnerabilities within an industry sector, such as chemical or petroleum sites. The American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPRA) developed the first version of the SVA methodology for the petroleum and petrochemical industry in 2003 (Moore, 2006).

The four-step approach of the SVA methodology can be described as follows:

1. Identify the critical asset and ascertain their added value to the system.
2. Assessment of threat sources (potential actions, capabilities and motivation).
3. Attractiveness analysis based on pairing of each critical asset with a threat source to identify potential vulnerabilities.
4. Scenario-based approach for risk assessment and countermeasure analysis.

There are many similarities between the many SVA methodologies available to risk managers. The RACAM project (2011) includes steps to identify processes and map assets (steps 2-3), these steps are reflected in the IDEFØ analysis (see D1.3). The fourth step in the RACAM method is to classify which assets are critical; this step is reflected in the SVA (step 1) methodology that has been adopted for this research. Step 1 (assess threats) of the RACAM method correlates directly with the SVA step 2 (threat sources) and RACAM's steps 5-6 (map attacks to assets and identify assets vulnerabilities) reflects step 3 of the SVA (critical assets

attractiveness); RACAM's steps 7-9 (identify existing controls, calculate residual risks and identify control options) correlates to step 4 of the SVA (the threat scenarios). Based on the RACAM recommendations the SVA methodology is in accordance with the design of threat scenarios and consistent with the IDEFØ analysis.

2.3 Reengineering the SVA: the THREAT Project methodology

The THREAT project methodology has been designed in two stages. A terrorist scenario design method was developed to 'originate and profile' a potential terrorist scenario. The Security and Vulnerability Assessment (SVA) methodology has been applied for the scenario designing in order to better identify their potential security failures and vulnerabilities. Finally, each developed scenario was assessed within the context of a previously identified terrorist MO to determine whether it was plausible and feasible as a potential hospital attack scenario.

2.4 Stage 1: Terrorist Scenario Design

Designing terrorist scenarios were first based on dedicated security and threats criteria. The design process to generate terrorist scenarios was tested and validated empirically at OSR. It is based on a four key actions:

1. Set up focus groups (with internal SMEs per Hospital Service or Function).
2. Review historical data on terrorist attacks (including criminality) and dynamics:
    - Attacks occurred in similar context (nation, area, cultural background);
    - Attacks occurred in different contexts;
    - Evaluate the adversary hazardousness with the following criteria:
        - Financial means (F)
        - Opportunities for people recruitment (P)
        - Knowledge acquisition (K)
        - Level of motivation (M)

          The threat ranking could be equal to $Tr = a1 * F + a2 * P + a3 * K + a4 * M$ with $a1 + a2 + a3 + a4 = 1$ and $F, P, K, M \in \{1, 2, 3, 4, 5\}$. Analytical Hierarchy Process (AHP) method could be used, in particular to determine the criteria weights a_i, as in the risk management system proposed by Vahdat et al.(2014).
    - Table 1 presents the terrorist profile, the threat history, the potential actions, the capability, the motivation, and the threat ranking Tr.

3. Brainstorming on hospital areas/functions (infrastructure services) by SMEs that are more likely to be exposed to a terrorist threat:

- Evaluate the weight of the hospital area/function (called critical asset) with the criteria below:
    - Added value (remuneration of economic activity or chargeback) to hospital (V)
    - Number of employees (E)
    - Cost of investment (C),

  The asset severity ranking could be equal to Ar = b1 * V + B2 * E + b3 * C with b1 + b2 + b3 = 1 and V, E, C $\in$ {1, 2, 3, 4, 5}. AHP method could also be used.
- Table 2 shows the critical assets of the hospital.
- Evaluate the attractiveness of the critical assets per adversary. Table 3 summarises this information.

4. Completion of the Threat Scenario Generator (TSG): the scenario reference table to model security and threats criteria consistently.

- Security criteria are:
    - Open public access
    - Structure/facilities damage
    - Access to radiological material
    - Access to OSR IT systems, including cyber access and physical access to servers and IT infrastructure
    - Conduct of animal research on site creating a target for animal activist groups
    - Access to biological material
- Threats criteria are:
    - Terrorist profile
    - Motivation
    - Modus operandi
    - Viable release of chemical, biological, radiological or nuclear material
    - Type and probability of collateral damage to OSR infrastructure and loss of life – impact to be measured by disruption to business
    - Security/safety barriers – extant measures to mitigate the risks

The TSG is described below in Table 4 and it was applied specifically to design nine terrorist scenarios for the OSR case studies and preliminary testing.

2.5 Threat Sources

Table 1: the Threat Sources

Adversary types	Source	Threat History	Potential actions	Adversary capability	Adversary motivation	Threat ranking
International terrorists	External/ Insider	• Missionary hospital, Jibla, Yemen, 30/12/02 • The Tikrit Hospital, Iraq, 2011 • Christian Worship Centre and hospital, Nwokyo, Nigeria, 15/04/14 • Christian hospital, Kabul, Afghanistan, 24/04/14 (Ganor and Halperin-Wernli, 2013)	• Armed assault • Hostage/Kidnapping • Bombing and damage/destruction of equipment and buildings • Loss of life • Release of CBRN material • Contamination of humans, equipment and buildings • Temporary disruption to hospital business • Long term disruption to hospital business	• High level of organisational support • Good financial backing • Network of members • Highly developed communications capabilities • Access to military grade weapons and explosives • Ability to improvise weapons and explosives	• Adversary is highly motivated (extremist) • Prepared to die for their cause • Intent to cause maximum damage to hospital assets including loss of lives and economic disruption	5

Table 1 provides threat source information that has been used to inform the TSG. The threat history provides information to highlight the potential for a hospital to be attacked, though the level of sophistication is constrained to the terrorist capability. The examples included in table 1 were unsophisticated armed attacks that were limited by the terrorist capability. It is highly plausible that an increase in terrorist capability worldwide could provide an enhanced attack methodology to include the use of ‘dirty bombs’ or other forms of CBRN material release.

THREAT ranking: in accordance with the literature review of terrorist attacks
1 less probable
5 most probable

2.6 Critical Assets

Table 2: the Critical Assets

Critical assets	Critically/Hazards	Asset severity Ranking
Emergency Department	The emergency department treats acute patients and then dispatches them to medical and surgical units. It is one of the main entrances to hospital. The Emergency department is the main actor for sustaining emergency management plans.	5
Operating rooms	The operating rooms are the main tool of surgical activities. They allow the diagnosis activity of medical activities. The operating rooms are the main source of added values for hospital activities.	4

ASSET SEVERITY ranking: in accordance with the criticality of the asset
1 less critical
5 most critical

2.7 Critical Asset Attractiveness

Table 3: Critical Assets Attractiveness

Critical assets	Critically/ Hazards	Asset Severity Ranking	Adversary types: International terrorist	Attractiveness ranking	Adversary types: Domestic terrorist	Attractiveness ranking	Adversary types: Employee	Attractiveness ranking
Emergency Department	The emergency department treats acute patients and then dispatches them to medical and surgical units. It is one of the main entrances to hospital. The Emergency department is the main actor for sustaining emergency management plans.	5	Major disruption of business activity; The entrance of patients in hospital is affected, several elected activities must be replaced by acute activities previously dedicated to Emergency department which is out of order; The emergency management plans become inactive.	5	Major disruption of business activity; The entrance of patients in hospital is affected, several elected activities must be replaced by acute activities previously dedicated to Emergency department which is out of order; The emergency management plans become inactive.	4		

ASSET SEVERITY ranking: in accordance with the criticality of the asset
1 less critical
5 most critical

2.8 Threat Scenario Generator

Table 4 : the Threat Scenario Generator

Scenario Code	Terrorist Profile	Motivation	Action/process	Hazard release	Type of damage	Security/safety barriers	Estimated Probability	Estimated Severity
			sequence of processes:				Risk index	Risk index
Scenario 1 Second Strike	Suicide bomber	Political/ religious	• A first terrorist strike occurs in Linate Airport • Emergency plan at Linate Airport is activated (EMS) • OSR responds with Hospital Emergency plan for massive influx of injuries activation and readiness • First patients enter the OSR ED: a green code arrived by a private car pretending to have been injured in Linate; when assessed shows a bomb-belt and detonates her/himself • The ED is damaged; some ED staff are seriously injured • OSR Internal Emergency Plan is activated to safeguard the rest of the hospital	Detonation and deflagration of facility	Human injuries and loss of life; destruction of building and facilities	Hospital Emergency Management Plan; monitoring of suspect behavior in ER; Procedures for internal terrorist threats and recognition of hazards		
Scenario 2 Open public access	Religious (Catholic) activist	Political/ religious	• An important Italian politician is in OSR for surgery in orthopedics; • She/he has just favored in Parliament the approval of a law in favor of abortion. • A "lone wolf"/small group of terrorists enters the hospital; gets access to the operating rooms. • Kills and seriously injuries the politician and some hospital personnel	Shooting	Loss of life and injuries	Access control systems; monitoring of suspect behavior; Procedures for internal terrorist threats and recognition of hazards		

Scenario Code	Terrorist Profile	Motivation	Action/process	Hazard release	Type of damage	Security/safety barriers	Estimated Probability	Estimated Severity
			sequence of processes:				Risk index	Risk index
Scenario 3 Structure/ facilities damage	Former OSR staff	Conflict with OSR/money topic (fired from hospital)	• A former OSR maintenance technician works as driver for an external ambulance service supporting the OSR; • Was fired by OSR and lost appeal to the court. • Being very disappointed against OSR, is approached by a member of an organisation (political, religious) and convinced to make an attack against the hospital upon payment of a lot of money. • Fabricates two rudimentary bombs and leaves one bomb in the ambulance with parking close to the first medical gas stock pile, the second one close to the second medical gas stock pile. • As he detonates the two bombs the OSR has no O2 flow anymore, except for the few O2 reservoirs available for emergency. • The Internal Emergency Plan is activated for transferring the patient dependent from O2	Detonation; deflagration of facility	Evacuation of OSR patients; damage to facilities and equipment	Access control systems; monitoring of suspect behavior; procedures for internal terrorist threats and recognition of hazards		

Scenario Code	Terrorist Profile	Motivation	Action/process	Hazard release	Type of damage	Security/safety barriers	Estimated Probability	Estimated Severity
			sequence of processes:				Risk index	Risk index
Scenario 4 Nuclear threat	Expert in nuclear material	Mercenary or by procurement	• An expert in nuclear material passes himself off as an employee of the hospital cleaning company. He can get access to the areas where a badge is necessary. • Can study all locations of the most dangerous radioactive materials and plan for a nuclear assault. • Targets the Irradiator Cesio 137, and one evening he gets there and easily steals the powder material. • Spreads the Cesio powder in the hospital and at his first radiation symptoms goes to the ED and explains what has done.	Spread of radioactive material	Irradiation of humans, facilities and equipment	Access control systems; monitoring of suspect behavior; procedures for internal terrorist threats and hazards recognitions; use of badge		
Scenario 5 Cyber attack	Expert in IT systems	Mercenary or by procurement	• An armed assault is conducted against the main IT repository and the server is destroyed. Among many sectors the Laboratory for Analysis is the most affected as it is dependent on the IT system. • The hospital has to face serious consequences	Sabotage of IT systems and hacking	Software and information communicatio n disruption and shut down	IT access systems; networks and hacking		

Scenario Code	Terrorist Profile	Motivation	Action/process	Hazard release	Type of damage	Security/safety barriers	Estimated Probability	Estimated Severity
			sequence of processes:				Risk index	Risk index
Scenario 6 Animal activists	Group of animal activists	Animal rights militant supporters	• A group of animalists makes a raid and gets access to the P3 animal facility • A number of animals are freed • Pictures and videos appear on internet pretending animals are HIV and hepatitis infected	Hacking and entering a private work area	Exposure to media of critical information	Hacking and access to restricted areas		
Scenario 7 Biological threat	Expert in biological technology	Human rights orthodox	A fake PhD researcher applies for internship in OSR Research Complex then: • enters the virus lab facility and collects SARS material, grows it, and puts it in a spray; • uses the virus lab facility to grow up a small Ebola sample sent from accomplices in West Africa; • buys genetic viruses parts (DNA viral) and with genetics' engineering techniques repeats the same actions and develops a new lethal virus composite. • Dressed as cleaner sprays over the surfaces of the most crowded area of the hospital (main acceptance area). • enters the TB laboratory and grows a particularly aggressive strain of TB and contaminates then the Centro San Luigi, full of HIV patients. Is a terrorist coming from a group against gay and HIV people.	Spread of viruses or other chemicals	Infection to humans, contamination of facilities and equipment	Hacking and access to restricted areas; production of illegal composites		

The name or numbering of each scenario listed in table 4 is defined together with a description of the potential terrorist profile and motivation to act intentionally (see the first three columns of Table 4). This process can take a simple approach describing the terrorist approach in general, but could be supported and enriched by additional research analysing terrorist attacks throughout the world since the attack on the World Trade Centre in New York during September 2001, an attack that is widely considered a defining moment in global terrorism and illustrated the level of violence that terrorists are willing to perpetrate.

The action process contained in column four is critical to understand the attack dynamics and actions with reference to the hospital systems involved. It is important that the analysis applied to this action/process be sufficient to identify whether the action/process is credible and feasible in relation to the actual events that have been generated. Another criterion is the plausibility of the simulated event, supported by historical evidence where this is possible even with reference to other healthcare environments and contexts or events that have occurred elsewhere. For example, there is no evidence to suggest a roving gunman attack has occurred at a hospital in the EU but events at the Charlie Hebdo magazine in Paris during 2015 demonstrate beyond doubt that terrorist have the appetite to methodically clear through target areas using military close quarter battle style techniques and they have access to firearms. When other incidents, such as the gang of 70 men whom rampaged through the Odense Hospital in Copenhagen in August 2012 (see D1.1) are considered, it only requires a small step to realise that hospitals could easily become targeted by terrorists.

Subsequent columns of hazard release, type of damage and Security/safety barriers should be formulated according to the terrorist profile as well as knowledge about the business processes, and safety and emergency procedures deployed by the hospital. It is to note that a description or model of the security barriers available and constraints could already provide future requirements to new and amended internal or external safety management procedures.

The last two columns of Table 4 (probability and severity) would provide a nominal risk quantification that will be discussed in greater detail in Stage 2: Scenario risk assessment.
Table 4 will be completed with countermeasures and best practices (security and safety barriers) in the deliverable 2 of WP3 which will analyse the internal and external management plans.

2.9 Stage 2: Scenario risk assessment

As a set of terrorist scenarios is being developed, some risk assessment knowledge is required to understand the implications of adverse events and the resulting impact of the scenario events.

The rationale for risk assessment stems out from a set of key functions. Computationally, the risk assessment serves the purpose to:

1. SCREEN and RANK scenarios for informed selection;
2. COMPARE terrorist scenarios for differential impacts and severity;
3. PRIORITISE major threats and inform decision maker for Cost Benefit Analysis (CBA)
4. PERFORM SENSITIVITY ANALYSIS towards risk reduction index;

And Operationally:

1. Provide the hospital with dedicated measures to prevent or minimize the impact of terrorist events;
2. Provide the hospital with reliable amendments for internal emergency plans;
3. Choose scenarios of major risk impact;
4. Propose risk based solutions with scenario analysis;
5. Inform the hospital about major security threats;
6. Inform the hospital about best possible resource management for optimal solutions.

The risk assessment approach applied to scenario estimations is based on best practices in hazard matrix applications (see Figure 1 of Deliverable 1.4: Risk Opportunity Map). Nevertheless an innovation has taken advantage of the criteria used for estimating the severity criterion. In particular, as a terrorist scenario is fully developed its likelihood as well as its severity is being estimated systematically and deeply. The combination of likelihood and severity shall provide an Index as best combination of both criteria.
The following THREAT Risk Matrix in Table 5 below has been developed through the collaboration of OSR and INSA de Lyon University. The matrix shows how the risk index shall be calculated on the 9 terrorist scenarios devised in Table 4.

Scenario n	Description		Severity				
		Likelihood	Infrastructure (physical) damages	Human Losses	Operational damages	Symbolic damages (media effect)	Mean severity
1	2 strikes: Linate airport + admission at Emergency Department	5	1	3	4	5	3,25
2	Attack against a VIP	5	2	2	2	5	2,75
3	Personal vengeance of a former employee - attack against medical gas facility	5	5	2	5	4	4
4	Fake employee stealing and using cesium powder	1	1	4	4	5	3,5
5	Cybercrime from an OSR competitor	5	1	1	3	2	1,75
6	Group of animalists willing to free the animals at P3 laboratory	3	1	1	4	5	2,75
7	Fake PhD researcher stealing an Ebola sample	1	1	5	5	5	4
8	Bacteriological attack against San Luigi (anti gay)	2	1	3	3	5	3
9	Water contaminated with cholera	1	5	1	5	4	3,75

Relative ranking	
1	Very low
2	Low
3	Medium
4	High
5	Very high

Table 5: THREATS Risk Matrix

In general the risk model assumed for the matrix in Table 5 above is the risk of *terrorist attack* modelled by formula: **R = L x S**, where the R risk is a weighted combination of the likelihood L (e.g., chance of occurrence from 1 to 5) and the severity of the hazard S (i.e., the impact of the terrorist attack).

Notably the following factors were considered for computation:

- No complete statistics are available to inform L or S values to improve their estimation;
- Expert Judgment is a robust baseline to estimate L and S;
- L is considered a single point estimator;
- S is a weighted linear combination of four different severity criteria.

The relative ranking both for L and S was initially a nominal value on a 5-point scale system ranging from 1 (very low) to 5 (very high). Nevertheless, a more reliable quantification for the various risk parameters has been suggested as shown in Annex 1. This should disambiguate and facilitate a more objective risk quantification.

A complementary approach to those suggested in Annex 1 in this Deliverable would be to model the parameters used to assess the risk and to compute the ranking as fuzzy values: as the events related to the scenarios are very rare and uncommon, it is hard to have a precise idea of their likelihood and their potential impacts. Generally speaking, risk modelling and assessment methodologies should be designed to handle uncertainty and subjectivity. Besides, the relative weights introduced in stage 1 to evaluate the features of the critical assets and the threat may vary and account for several expert opinions, which are sometimes based on imprecise and uncertain judgment. This could advocate for the use of fuzzy multi-criteria decision making (MCDM) methods, as in Vahdat et al. (2014).

The final and complete results of the risk assessment for each scenario will be published in D3.2.

3. Analysis of the “as-is” system: static modelling

3.1 Methodologies dedicated to Health Care

Since there is no particular modelling approach dedicated to vulnerability analysis, a selection of methodologies coming from industrial management that were already applied to health care sectors has been listed in this work. Among the enterprise modelling languages, there are the IDEF family languages that have been developed by the Integrated Computer Aided Manufacturing (ICAM) program. Ducq et al. (2004) uses IDEFØ to describe the different processes within a hospital. This method is useful in order to specify the ‘as-is’ situation of a system during a business process reengineering (BPR) approach (Kim and Jang, 2002). Unified Modelling Language (UML) is a standardised specification language for object modelling. It fits for the analysis and design of information systems. It was used by Staccini et al. (2001) to create a data model for the blood transfusion process. ARIS, along with ARIS toolset, is an engineering tool based on modelling languages, using a process view. It allows representation of the different views of an enterprise (functional, information, organisational and control) based on different levels (conceptual, technical and implementation). It enables the modelled processes to be simulated. Chen et al. (2015) used ARIS to model an Emergency Management Plan for a hospital evacuation. The GRAI Integrated Methodology (GIM) has been developed by the Grai Laboratory of the University of Bordeaux in France (Doumeingts et al., 2000). It combines the capabilities of decision modelling, information modelling, process modelling and physical modelling. Different modelling languages are used like IDEFØ, the GRAI grid and MERISE. GIM were applied in different projects in order to set up a decision and control system in hospitals (Besombes et al., 2014; Besombes et al., 2004; Ducq et al., 2004). Analysing, Specification, Design and Implementation (ASDI) methodology developed by Gourgand and Kellert (1992) is an open integrated environment of proven methods and tools helping in the gathering and documentation of knowledge to model and simulate production systems. ASDI was used during the setup of a new hospital in France to model and simulate the health care supply chain and for reengineering and evaluating the supply chains of existing hospitals (Di Martinelly et al., 2011; Chabrol et al., 2011). The ASDI methodology uses tools like ARIS and UML to define and to detail the processes. Process-oriented methods are widely used in health care engineering but they are only used on a limited number of processes.

3.2 IDEFØ/SADT methods

The Structured Analysis Design Technique (SADT) method uses a standard graphical language of communication (Ross, 1977). It facilitates the modelling of an existing (as-is) or future (to-be) system, to understand its activities. The structure and abstraction of SADT allow easier understanding of complex systems, and a top-down modular analysis. The analysis of the system is represented as a collection of hierarchically organised diagrams with a limited number of elements. This model could focus on the activities of the analysed system, represented by the actigrams or the data that the system needs to process, represented by the datagrams, in a tree structure of the system. Figure 1 illustrates the principle of hierarchical decomposition and the formalism of the diagrams.

The symbolism uses boxes that have different meanings according to the two approaches (activity or data) and arrows which define flows or actions respectively to the selected approach. The activity approach favours the appearance of events (Guinet, 1990), while data approach (less used) promotes the appearance of objects. Validation of knowledge is done through a reader-writer process, which supports communication between analysts and users.

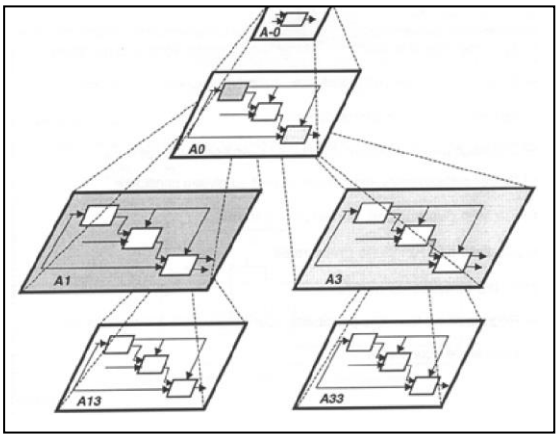

Figure 1: Hierarchical decomposition

IDEFØ (1993) is a method designed to model the decisions, data and activities of an organisation or system. IDEFØ was derived from SADT. The United States Air Force commissioned the authors of SADT to develop a functional modelling method for analyzing and communicating the functional perspective of a system.
(See http://www.idef.com/IDEF0.htm).

Visio Professional 2010 provides several flowchart templates; one of them supports the IDEFØ Diagrams.
(See http://office.microsoft.com/en-us/visio-help/create-idef0-diagrams-HP001208587.aspx).
The IDEFØ model helps to organise the analysis of an existing system and allows the promotion of good communication between the analysts and the users. IDEFØ enables an easier understanding of complex systems by a gradual approach of its complexity. As a communication tool, it enhances user involvement and allows obtaining consensus models (Bevilacqua et al., 2012). With relevance to this work, IDEFØ will assist in identifying units' accessibility and the propagations of flows. An IDEFØ model will be first created for the hospital analysis and then it will be used as a static model which will represent the basic information to generate a dynamic model, for example a flow model to calculate patient traffic or infected patients passing a contaminated area.

OSR covers an area of about 300 thousand square meters and is composed of 11 buildings that accommodate 49 specialty clinics with over 6,000 employees. A first physical decomposition of the hospital to buildings and later of the buildings to floors has been made (Figures 2-13). A second functional decomposition of some care units located at the leaves of the previous tree has been done (figures 14-17), it represents care processes which are considered to be critical (i.e. the emergency department).

3.3 Physical view of “as-is” model of OSR with IDEFØ

This IDEFØ model includes several types of flows: patients and visitors (in red), staff (in green), vehicles (in blue) and others (in black).

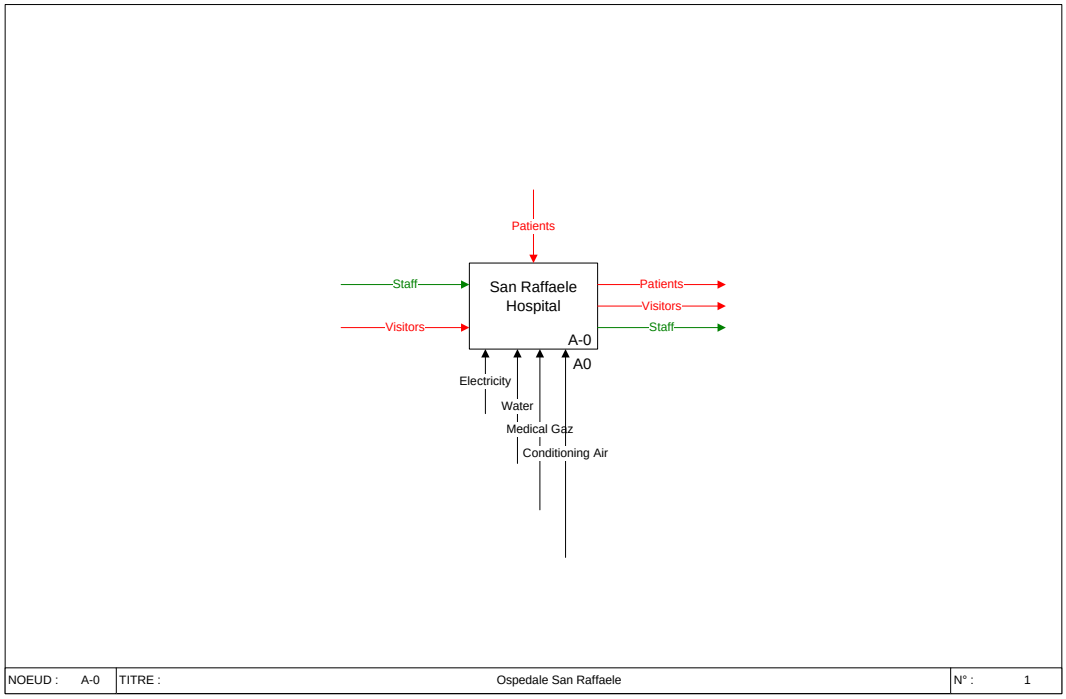

Figure 2: The context diagram to model the flow exchange between OSR and its environment.

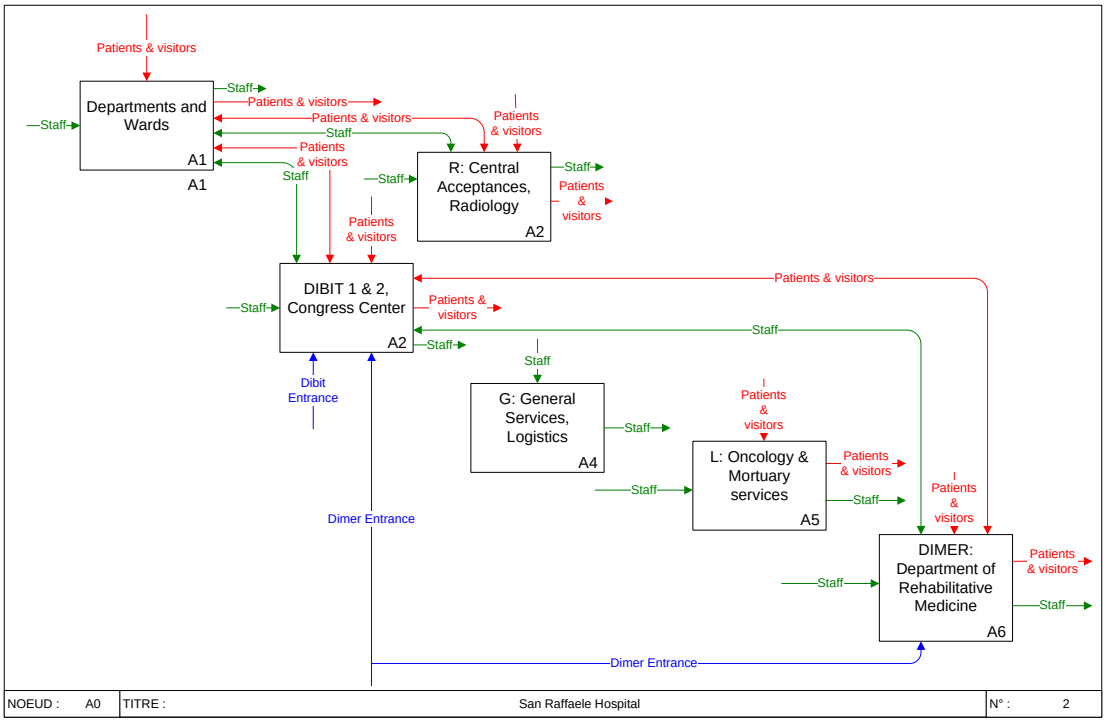

Figure 3: First child diagram for modelling the flow exchange between main buildings.

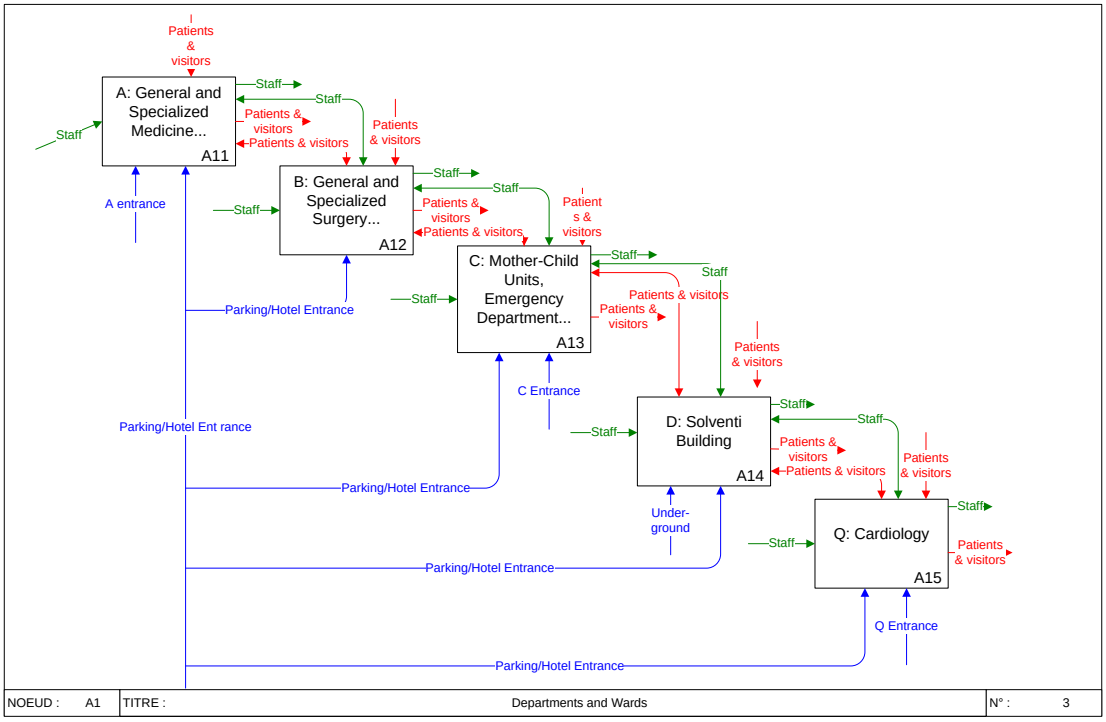

Figure 4: Child diagram A1 for modelling the main house that consists of 5 connected buildings.

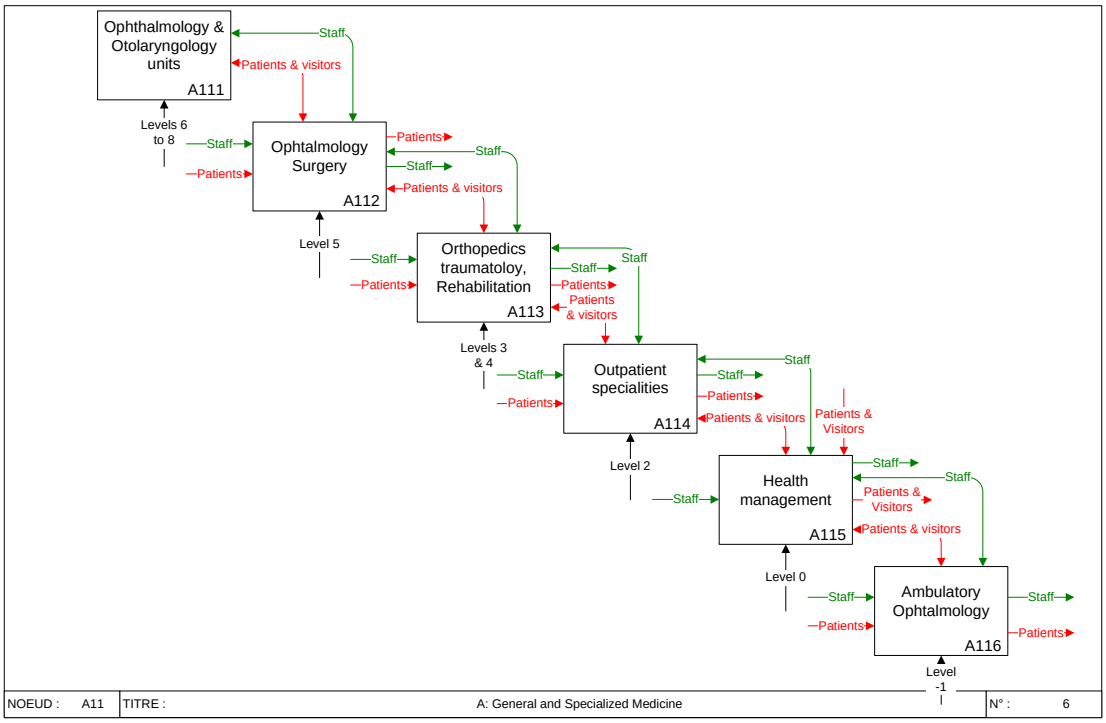

Figure 5: Child diagram A11 for modelling the flows of building A.

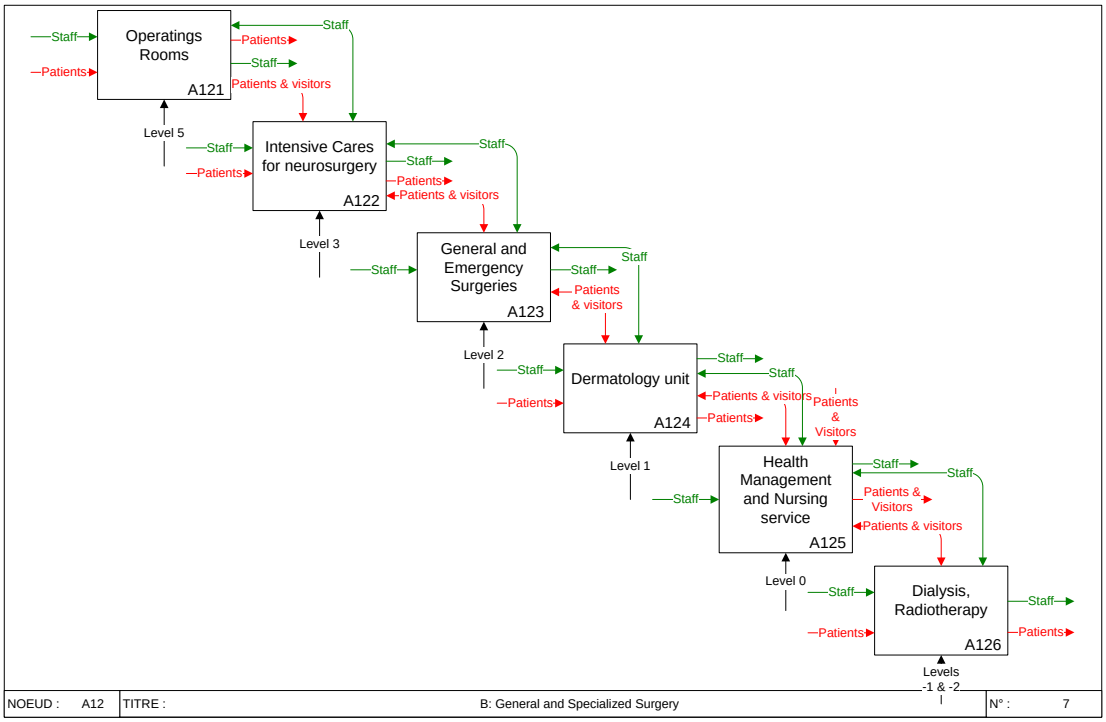

Figure 6: Child diagram A12 for modelling the flows of building B.

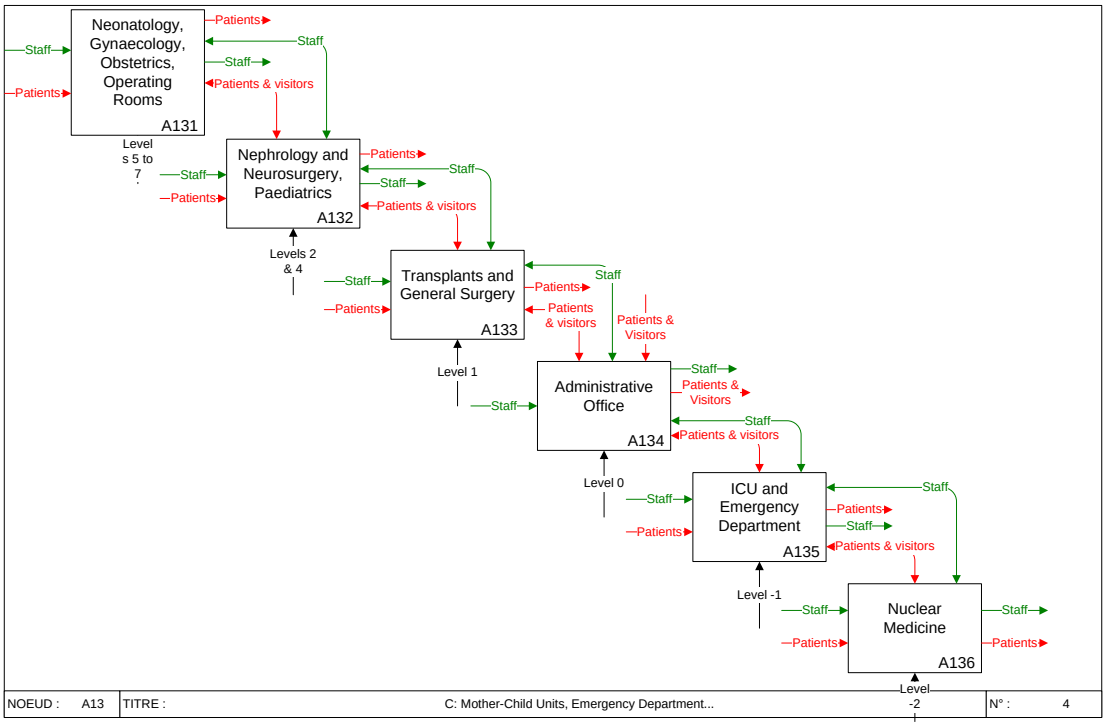

Figure 7: Child diagram A13 for modelling the flows of building C.

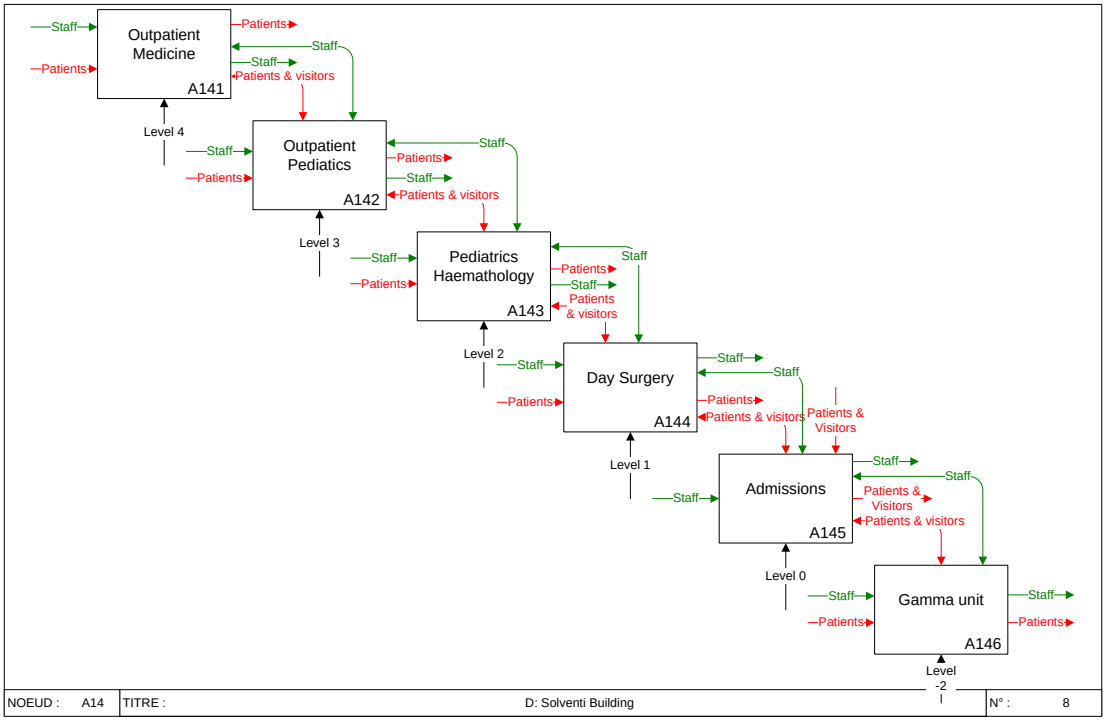

Figure 8: Child diagram A14 for modelling the flows of building D.

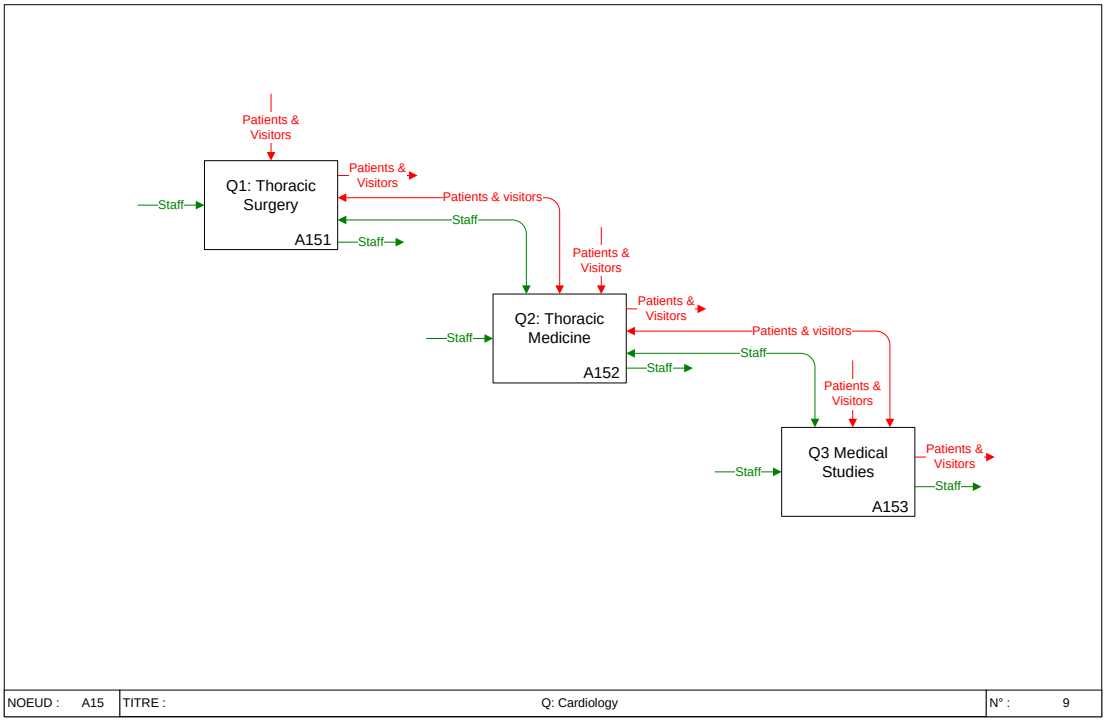

Figure 9: Child diagram A15 for modelling the building Q that is composed of 3 sub-buildings.

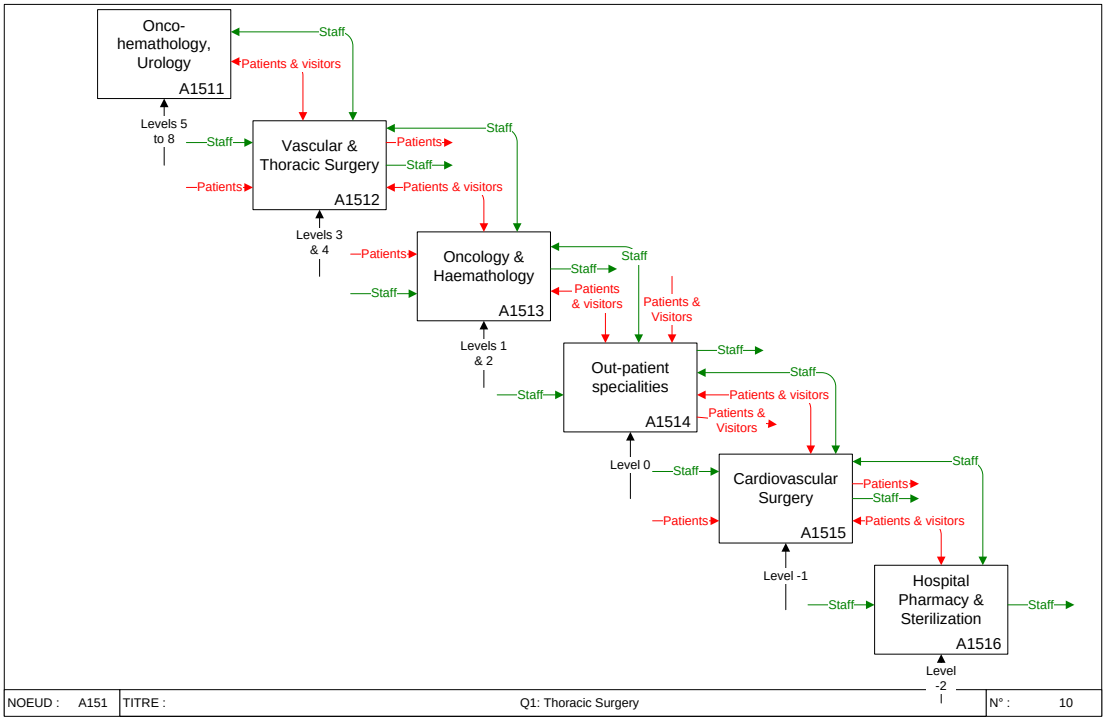

Figure 10: Child diagram A151 for modelling the flows of building Q1.

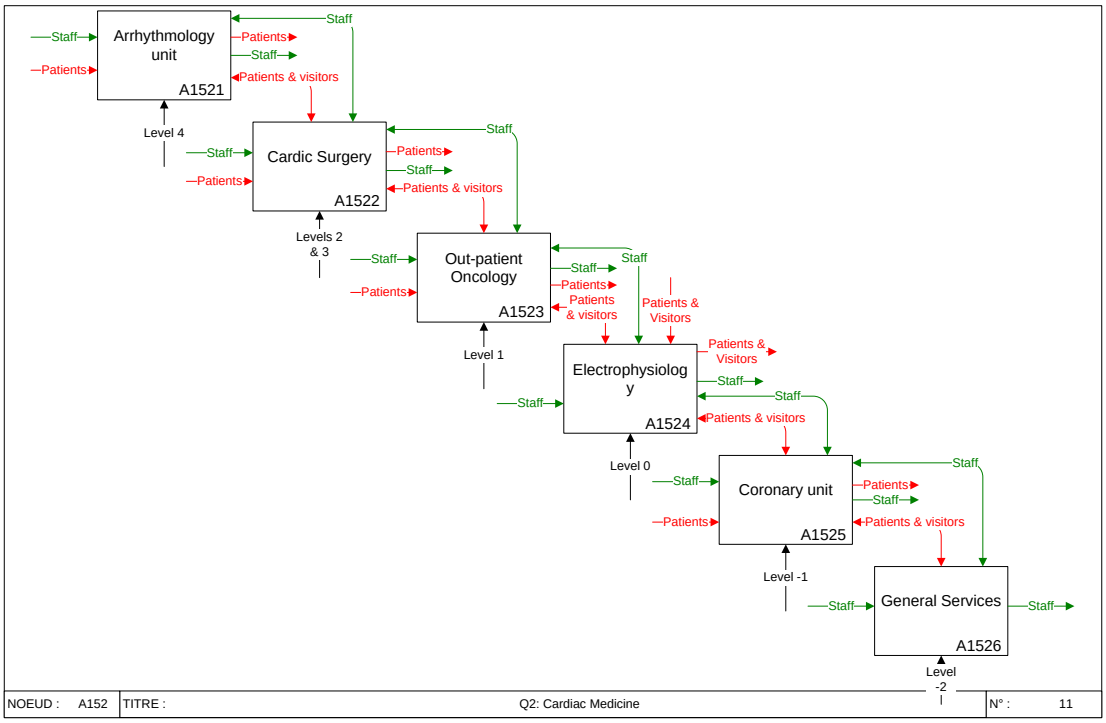

Figure 11: Child diagram A152 for modelling the flows of building Q2.

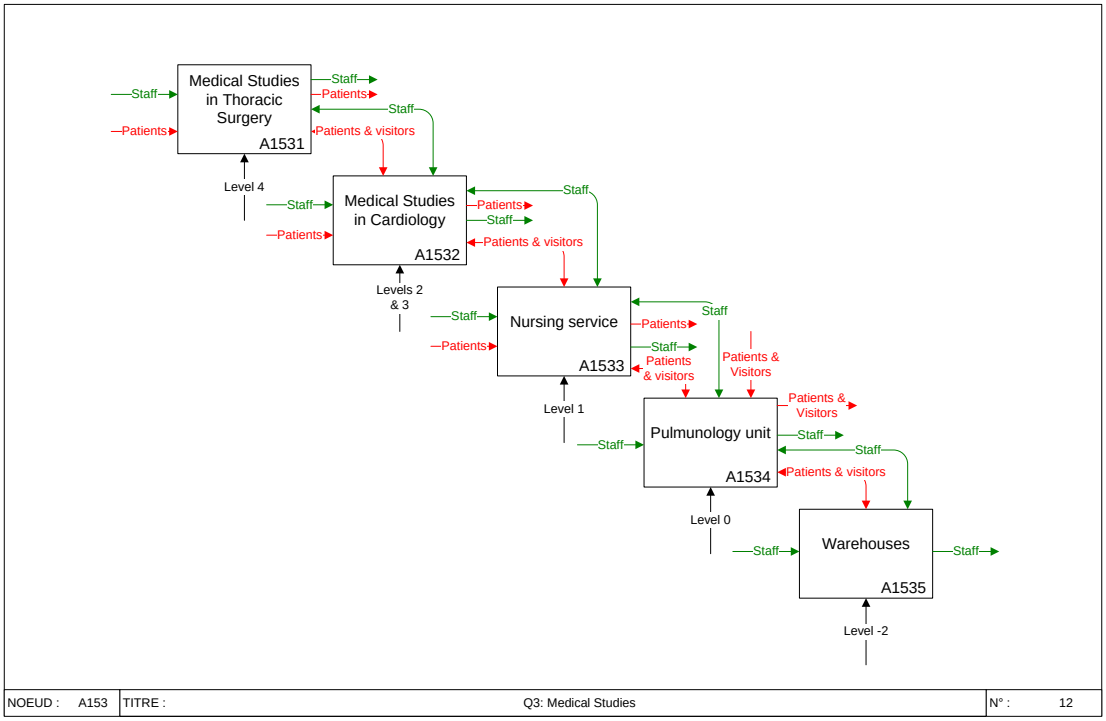

Figure 12: Child diagram A153 for modelling the flows of building Q3.

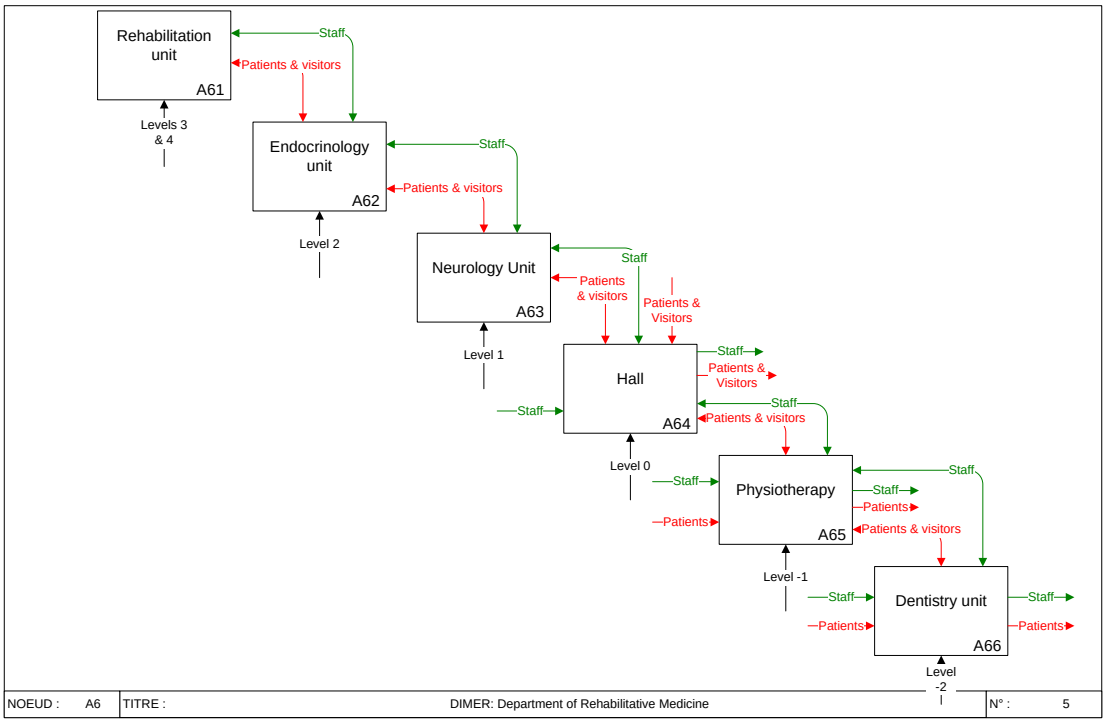

Figure 13: Child diagram A6 for modelling the flows of building DIMER.

3.4 Functional view of “as-is” model of Emergency Department with IDEFØ

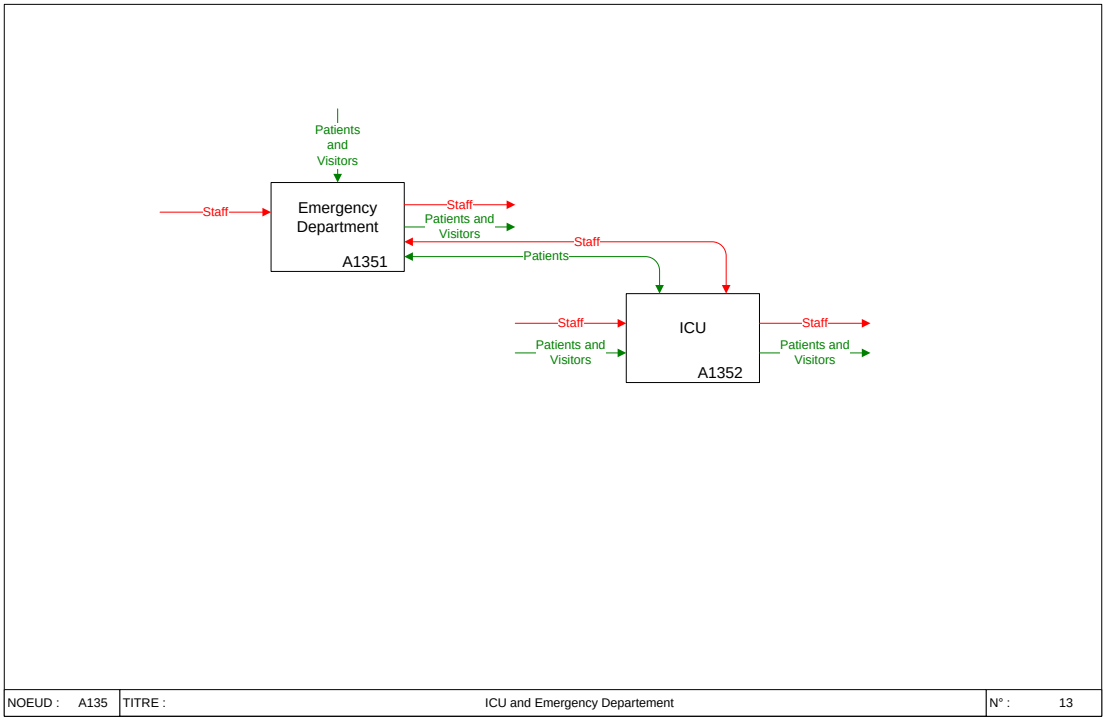

Figure 14: Child diagram A135 for modelling the Emergency Department

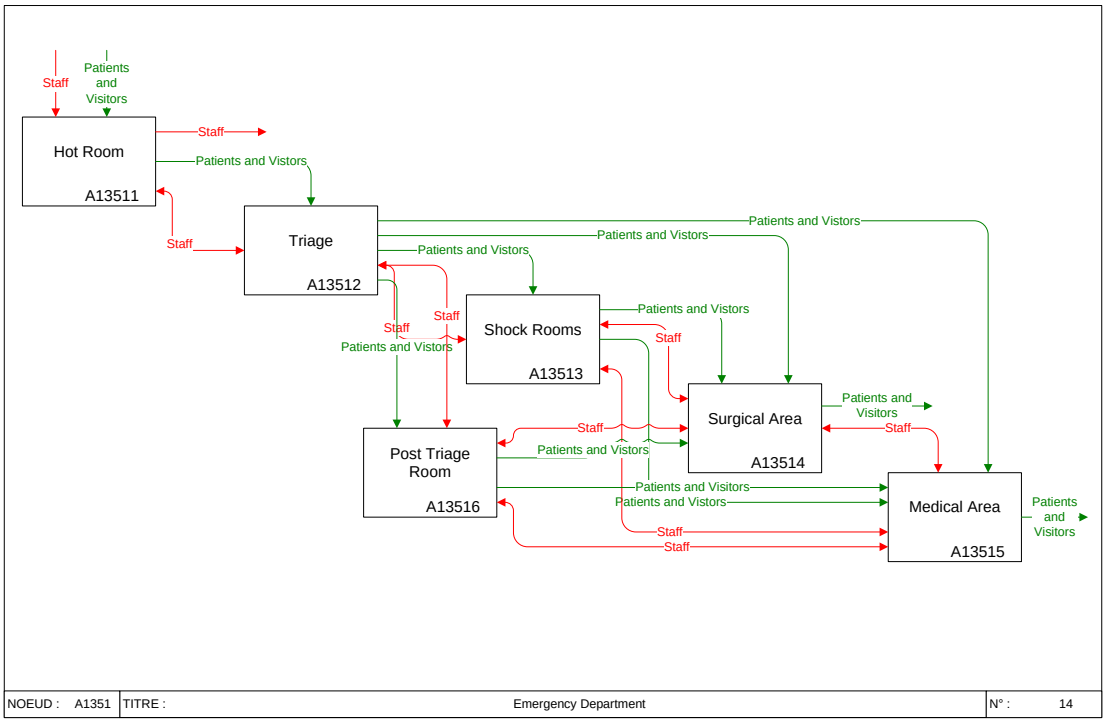

Figure 15: Child diagram A1351 for modelling the flows of the Emergency Department.

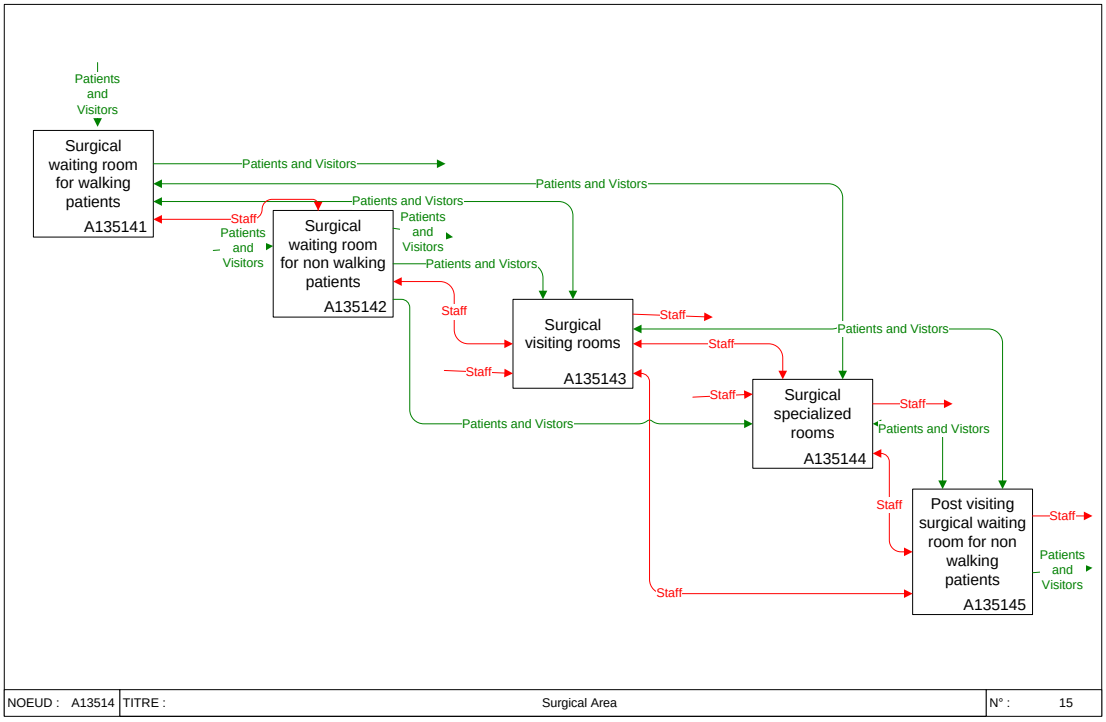

Figure 16: Child diagram A13514 for modelling the flows of the patients needing surgical treatments.

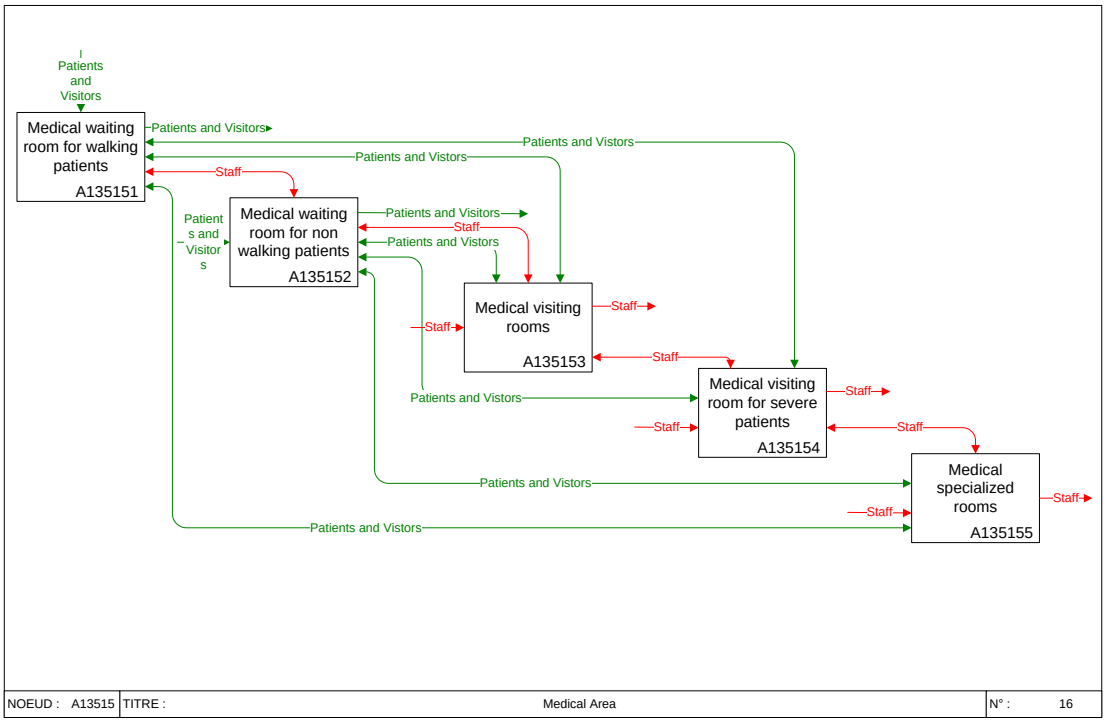

Figure 17: Child diagram A13515 for modelling the flows of the patients needing medical treatments.

Figure 2 is the top view of the OSR model, it represents the environment of the hospital with different input and output flows. Figure 3 is the child-diagram of the previous diagram called father-diagram, it shows that the hospital is composed of a core building called “Departments and wards” and of five other isolated buildings: Dibit, Dimer, G, L and R. External flows around buildings are modelled. Figure 4 details the box called “Departments and wards”, specifying that it is composed of five others linked buildings: A, B, C, D and Q. These buildings are connected by corridors open to staff, patients and visitors. The vehicle external accesses are also represented. Figures 5 to 9 details each of the previous buildings, they model the care units or services located at the different floors and linked by stairways and lifts. The links between twin buildings (A and B, B and C, C and D, D and Q) are also specified per floor. Figures 10 to 12 detail the building Q, which is composed of 3 twin buildings. Figure 13 shows the structure of the Dimer Building. All these diagrams allow us to model the structure of the buildings of the hospital, detailing the different internal and external accesses per floor, where care units or sets of care units are located (Figure 14) i.e. the critical asset location. Figures 15 to 17 model the processes of one of the main critical assets: the Emergency Department that controls the Emergency Management Plans for OSR. The patient path is specified across resources. For coherence reasons, the names of rooms are used instead of the names of the medical/surgical activities, but each room is dedicated to medical or surgical activities. The common patient path is represented on Figure 15. The dedicated patient paths are shown in Figures 16 and 17 respectively for surgical and medical activity requirements.

The “as-is” model enables the THREATS Critical Pillars to be represented, which have been defined by work-package 1. The physical view focuses on infrastructures and humans. The boxes represent whole or part of infrastructures and most of the flows are dedicated to humans: patients, visitors, staff, etc.

Regarding to the functional view, the processes of critical assets are modelled, and the boxes represent processes or activities. The mechanism arrows (the arrows arriving under the boxes) of IDEFØ that specify non-consumable resources, enable the modelling of inputs, outputs, storages of information which are the third pillar.

3.5 Analysis of the “as-is” system: dynamic modelling

3.5.1 Context

The physical view of the ‘as-is’ model is composed of 12 diagrams of activities (Figures 2-13). The decomposition tree is of four levels and has 47 leaves which represent 47 sets of services/units. 199 direct accesses between sets of services/units have been modelled. Four other diagrams (Figure 14-17) of activities allow for the modelling of the processes of the Emergency department which defines a critical asset regarding emergency management plans. The physical view shows a picture of the hospital. In order to study the dynamic of the ‘as-is’ system (i.e. to create a movie of the hospital), a first simulation tool must be designed. Before studying the different scenarios of terrorist attacks, it was agreed to study the patient traffic in the hospital in order to identify the most crowded places which could be the most vulnerable places due to concentration of population (D1.3). First we export from the IDEFØ model the different accesses between the leaves (services/units) of the decomposition tree of the physical view. The result is modelled by the Acc matrix (Table 6) where the lines/columns represent the leaves and the intersections between lines and columns identify presence/absence of a direct access. This matrix could be translated to a graph and a flow problem could be studied on this graph. In defining on one hand the patient inputs to the hospital and on the other hand the care units appointments, which are both located at leaves of the ‘as-is’ model, the hospital entrance flows could be studied. In defining on one hand the patient exits of the hospital and on the other hand the care units discharges, which are both located at leaves of the ‘as-is’ model, the hospital departures could also be studied. These two flow problems have been modelled by a linear program. The Cplex solver has been chosen to solve it. Firstly the linear problem is presented, secondly the access matrix Acc and finally the results given by Cplex with a single entrance (from subway) and for several entrances.

3.5.2 Problem

Parameters

N: number of services/units (number of leaves of IDEFØ tree),

i,j: unit indices,

Acc(i,j): If it is equal to 1 there is an access to go directly from unit i to unit j, 0 otherwise; the accesses are extracted from the IDEFØ model (Table 6),

Input(i): Number of people (patients and visitors) incoming in i directly from outside (entry point),

Output(i): Number of people (patients and visitors) admitted in i (care unit),

Variables

XG(i,j): Number of people going from i to j,

XR(i,j): Number of people returning from i to j,

3.5.3 Model

Objective function:

$$Minimiser\ Z = \overbrace{\sum_{i=1}^{N}\sum_{j=1}^{N}(XG(i,j)+XR(i,j))}^{Traffic} \quad [1]$$

Constraints:

$$\sum_{j=1|j\neq i}^{N} XG(\mathrm{j,i})*\mathrm{Acc(j,i)} - \sum_{j=1|j\neq i}^{N} XG(\mathrm{i,j})*\mathrm{Acc(i,j)} + Input(i) - Output(i) = XG(i,i) \quad \forall i = 1,...,\mathrm{N} \quad [2]$$

$$\sum_{j=1|j\neq i}^{N} XR(\mathrm{j,i})*\mathrm{Acc(j,i)} - \sum_{j=1|j\neq i}^{N} XR(\mathrm{i,j})*\mathrm{Acc(i,j)} - Input(i) + Output(i) = XR(i,i) \quad \forall i = 1,...,\mathrm{N} \quad [3]$$

$$XG(i,\mathrm{j}) \geq 0 \qquad \forall i = 1,...,\mathrm{N} \quad \forall j = 1,...,\mathrm{N} \quad [4]$$

$$XR(i,\mathrm{j}) \geq 0 \qquad \forall i = 1,...,\mathrm{N} \quad \forall j = 1,...,\mathrm{N} \quad [5]$$

Comments

This linear program minimises the traffic of the whole hospital (equation 1). In equations 2, the remaining flow of unit i is equal to the flow entrances from neighborhood units minus flow exits to neighborhood units plus the outside entrances minus the outside exits. Equations 2 are conservation flow constraints; they model the remaining flow for incoming people. Equations 3 are the opposite equations of equations 2; they are also conservation flow constraints, they model the remaining flow for returning people. The hypothesis that the sum of entrances is equal to the sum of exits (∑ Input(i) = ∑ Output(i)), is retained. Under this hypothesis, respecting the demands (Output(i)) and the supplies (Input(i)) the remaining flows of units will be equal to zero.

The total traffic of unit i is equal to the input traffic from inside, plus the output traffic to inside, plus the maximum between the entrances from outside and the exits to outside: $Traffic = \sum_{j=1|j\neq i}^{N} XG(\mathrm{j,i}) + \sum_{j=1|j\neq i}^{N} XR(\mathrm{j,i}) + Maximum(Input(i), Output(i))$.

If patients must pass through a compulsory place i (i.e. an admissions unit), we add the constraint:

$$\sum_{j=1|j\neq i}^{N} XG(\mathrm{j,i})*\mathrm{Acc(j,i)} \geq \sum_{j=1}^{N} Input(\mathrm{j})$$

Extensions

The dynamic model of OSR represents 47 units or services modelled by IDEFØ boxes located at the leaves of the decomposition tree. Solving the traffic problem leads to 4,419 decision variables and 94 constraints. The extension of the model for several periods (a 10 hour horizon with steps of one hour) could lead to a huge but feasible model. For a study of more periods (a week) a sequential use of the basic model per day could be effective. Input and output parameters could be easily calculated over the week horizon taking into account the length of stay, and the use of the basic model for each day of the horizon will allow us to have a good idea of the hospital traffic. The dummy sources or the dummy sinks could be used to model units' capacities and as result the waiting patients or the delayed patients. Consequently, the “going” and “returning” constraints will have dedicated parameters which will vary per day.

The extension of our model to different kinds of people could be possible if it is limited to 2 or 3 types i.e.: inpatients, outpatients and visitors. For external emergency management plans, we can model them by parameters such as: inputs and outputs (the red patients, yellow patients and green patients), the accesses (units' access reorganization) and capacities (unit’s staff). With or without a sequential use of our daily model, the increasing of units' capacities and the exits to foreign hospitals (dummy sinks) could be integrated.

OSR's Matrix of accesses (Table 6: Acc parameters)

	A111	A112	A113	A114	A115	A116	A121	A122	A123	A124	A125	A126	A131	A132	A133	A134	A135	A136	A141	A142	A143	A144	A145	A146	A1511	A1512	A1513	A1514	A1515	A1516	A1521	A1522	A1523	A1524	A1525	A1526	A1531	A1532	A1533	A1534	A1535	A61	A62	A63	A64	A65	A66	
A111	1	1																																														A111
A112	1	1	1			1																																										A112
A113		1	1	1			1																																									A113
A114			1	1	1			1																																									A114
A115				1	1	1				1																																							A115
A116					1	1					1																																				1		A116
A121		1					1	1				1																																					A121
A122			1				1	1	1				1																																				A122
A123				1				1	1	1			1																																				A123
A124									1	1	1			1																																				A124
A125					1					1	1	1			1																																		A125
A126						1					1	1				1	1																																A126
A131							1						1	1																																			A131
A132								1	1				1	1	1				1	1	1																											A132
A133										1				1	1	1						1																											A133
A134											1				1	1	1						1																											A134
A135												1				1	1	1																															A135
A136												1					1	1						1																									A136
A141													1						1	1					1																									A141
A142													1						1	1	1				1																									A142
A143													1							1	1	1				1																									A143
A144														1							1	1	1			1																									A144
A145															1							1	1	1			1																									A145
A146																								1																											A146
A1511																									1	1																									A1511
A1512																									1	1	1																									A1512
A1513																											1	1																									A1513
A1514																												1																									A1514
A1515																													1																									A1515
A1516																														1																									A1516
A1521																															1																									A1521
A1522																															1	1																									A1522
A1523																																1																									A1523
A1524																																	1																									A1524
A1525																																		1																									A1525
A1526																																			1																									A1526
A1531																																				1																									A1531
A1532																																					1																									A1532
A1533																																						1																									A1533
A1534																																							1																									A1534
A1535																																								1																									A1535
A61																																									1	1																									A61
A62																																									1	1	1																									A62
A63																																											1	1	1																									A63
A64																																													1	1	1																									A64
A65						1																																									1	1	1																									A65
A66																																																1	1																									A66
	A111	A112	A113	A114	A115	A116	A121	A122	A123	A124	A125	A126	A131	A132	A133	A134	A135	A136	A141	A142	A143	A144	A145	A146	A1511	A1512	A1513	A1514	A1515	A1516	A1521	A1522	A1523	A1524	A1525	A1526	A1531	A1532	A1533	A1534	A1535	A61	A62	A63	A64	A65	A66	

OSR’s Matrices of traffic with a single entrance and exit from A145 of building D (Table 7: XG and XR results)

	A111	A112	A113	A114	A115	A116	A121	A122	A123	A124	A125	A126	A131	A132	A133	A134	A135	A136	A141	A142	A143	A144	A145	A146	A1511	A1512	A1513	A1514	A1515	A1516	A1521	A1522	A1523	A1524	A1525	A1526	A1531	A1532	A1533	A1534	A1535	A61	A62	A63	A64	A65	A66	
A111	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A111
A112	500	0	550	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A112
A113	0	550	0	1050	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A113
A114	0	0	1050	0	1550	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A114
A115	0	0	0	1550	0	0	0	0	0	0	4550	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A115
A116	0	0	0	0	3000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2500	0	A116
A121	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A121
A122	0	0	0	0	0	0	50	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A122
A123	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A123
A124	0	0	0	0	0	0	0	0	50	0	550	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A124
A125	0	0	0	0	1550	0	0	0	0	550	0	3050	0	0	0	5150	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A125
A126	0	0	0	0	0	3000	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A126
A131	0	0	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A131
A132	0	0	0	0	0	0	0	100	0	0	0	0	50	0	1150	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A132
A133	0	0	0	0	0	0	0	0	0	0	0	0	0	1150	0	1200	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A133
A134	0	0	0	0	0	0	0	0	0	0	5150	0	0	0	1200	0	100	0	0	0	0	0	6450	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A134
A135	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A135
A136	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A136
A141	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A141
A142	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A142
A143	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	1000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A143
A144	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1000	0	3150	0	0	0	2100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A144
A145	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6450	0	0	0	0	0	3150	0	100	0	0	0	600	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A145
A146	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A146
A1511	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1511
A1512	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	1050	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1512
A1513	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2100	0	0	0	1050	0	0	0	0	0	50	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1513
A1514	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	600	0	0	0	0	0	550	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	A1514
A1515	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	550	0	0	0	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	A1515
A1516	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1516
A1521	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1521
A1522	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1522
A1523	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1523
A1524	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	A1524
A1525	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1525
A1526	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1526
A1531	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1531
A1532	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1532
A1533	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1533
A1534	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	A1534
A1535	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1535
A61	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	0	0	0	A61
A62	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	1000	0	0	0	A62
A63	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1000	0	1500	0	0	A63
A64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1500	0	1500	0	A64
A65	0	0	0	0	0	2500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1500	0	500	A65
A66	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	A66
	A111	A112	A113	A114	A115	A116	A121	A122	A123	A124	A125	A126	A131	A132	A133	A134	A135	A136	A141	A142	A143	A144	A145	A146	A1511	A1512	A1513	A1514	A1515	A1516	A1521	A1522	A1523	A1524	A1525	A1526	A1531	A1532	A1533	A1534	A1535	A61	A62	A63	A64	A65	A66	

The patient flows go from D to C, from C to B, from B to A, from A to DIMER on one hand and from D to Q1 and Q1 to Q2 on the other hand using all levels. The most crowded place received 6,450 visits.

OSR's Matrices XG + XR of traffic with several entrances and exits (Table 8: XG and XR results)

	A111	A112	A113	A114	A115	A116	A121	A122	A123	A124	A125	A126	A131	A132	A133	A134	A135	A136	A141	A142	A143	A144	A145	A146	A1511	A1512	A1513	A1514	A1515	A1516	A1521	A1522	A1523	A1524	A1525	A1526	A1531	A1532	A1533	A1534	A1535	A61	A62	A63	A64	A65	A66	
A111	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A111
A112	500	0	550	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A112
A113	0	550	0	1050	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A113
A114	0	0	1050	0	1550	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A114
A115	0	0	0	1550	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A115
A116	0	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A116
A121	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A121
A122	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A122
A123	0	0	0	0	0	0	0	0	150	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A123
A124	0	0	0	0	0	0	0	150	0	650	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A124
A125	0	0	0	0	0	0	0	0	650	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A125
A126	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A126
A131	0	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A131
A132	0	0	0	0	0	0	0	0	0	0	0	0	50	0	1050	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A132
A133	0	0	0	0	0	0	0	0	0	0	0	0	600	0	1100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A133
A134	0	0	0	0	0	0	0	0	0	0	0	0	0	650	0	100	0	0	0	0	0	0	450	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A134
A135	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A135
A136	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A136
A141	0	0	0	0	0	0	0	0	0	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A141
A142	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	450	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A142
A143	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	950	0	1000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A143
A144	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1450	0	1050	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A144
A145	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1500	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A145
A146	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A146
A1511	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1511
A1512	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	550	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1512
A1513	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	550	0	1050	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1513
A1514	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1050	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1514
A1515	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1515
A1516	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1516
A1521	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1521
A1522	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	550	0	0	0	0	0	0	0	0	0	0	0	0	0	A1522
A1523	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	550	0	1050	0	0	0	0	0	0	0	0	0	0	0	0	A1523
A1524	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1050	0	500	0	0	0	0	0	0	0	0	0	0	0	A1524
A1525	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	0	0	0	0	0	0	0	0	0	0	0	A1525
A1526	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1526
A1531	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1531
A1532	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1532
A1533	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1533
A1534	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1534
A1535	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A1535
A61	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	0	0	0	A61
A62	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	0	1000	0	0	A62
A63	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1000	0	1500	0	A63
A64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1500	0	1000	A64
A65	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1000	0	A65
A66	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	500	A66

The patients use the direct entrances and exits of each building at level 0 to reach all other levels. The most crowded places received 1,550 visits.

The linear program has been solved with Cplex [IBM ILOG CPLEX] for 47 care-units, which leads to 94 constraints and 4,419 variables, in order to check the accuracy of the equations. Some experiments have been made to calculate the hospital traffic in order to assess this dynamic approach and to evaluate the integration link between the static and dynamic models. The values of entrances (input) and of admissions (output) are given in Table 9 for the incoming traffic. These values are reversed for the leaving traffic: people incoming (output) and people leaving (input). Entrances and exits are calculated from care unit admissions with the hypothesis that people using the direct outside accesses of the care unit building.

PEOPLE INCOMMING				PEOPLE LEAVING			
A111	0	A1511	0	A111	500	A1511	500
A112	0	A1512	0	A112	50	A1512	50
A113	0	A1513	0	A113	500	A1513	500
A114	0	A1514	1100	A114	500	A1514	0
A115	2050	A1515	0	A115	0	A1515	50
A116	0	A1516	0	A116	500	A1516	0
A121	0	A1521	0	A121	50	A1521	500
A122	0	A1522	0	A122	50	A1522	50
A123	0	A1523	0	A123	50	A1523	500
A124	0	A1524	1550	A124	500	A1524	0
A125	700	A1525	0	A125	0	A1525	500
A126	0	A1526	0	A126	50	A1526	0
A131	0	A1531	0	A131	50	A1531	0
A132	0	A1532	0	A132	500	A1532	0
A133	0	A1533	0	A133	50	A1533	0
A134	750	A1534	50	A134	0	A1534	50
A135	0	A1535	0	A135	100	A1535	0
A136	0	A61	0	A136	50	A61	500
A141	0	A62	0	A141	500	A62	500
A142	0	A63	0	A142	500	A63	500
A143	0	A64	2500	A143	500	A64	0
A144	0	A65	0	A144	50	A65	500
A145	1600	A66	0	A145	0	A66	500
A146	0			A146	50		

Table 9: Input and output parameters

The computation time is around 6 seconds and we have a traffic in hospital of 90,700 crossings (for a single access from the subway) and 40,700 crossings (for several accesses from external entrances/exits of each building), on the different corridors through the different accesses of OSR. The most crowded place receives 6,450 visits with a single access to hospital and 1,550 visits with several accesses to hospital.

Regarding the results (Tables 7 and 8), patients whom go directly to the care-unit building or outside when they can, coming from and for returning to outside. The crossings between buildings are very limited for the several-access case, but widely used for the single-access case. The stairways or the lifts are mainly used.

4. Conclusion

The scenario design involving terrorist attacks were studied to understand feasibility and applicability of various measures. Deliverable 1.3 of WP1 (DR/1/003, 2015) has been taken into account as source material to design and then develop an evolution of the SVA methodology.

The THREATS approach to modelling and developing preventive or risk reducing measures has shown to be successful in devising a set of tools to quantify and increase risk intelligence in case of terrorist attacks on hospitals. The assessment of risks and implications of nine different scenarios is now under evaluation.

The modelling approach described in this paper was based on OSR Hospital, which is fundamentally an open space. This is almost the most important vulnerability recognized: a lot of entrances without control, a lot of traffic of people and vehicles with poor security measures, several crowded areas and no plan how to control the crowd. Other vulnerabilities recognized are:

- The presence itself of hazards inside the hospital (like nuclear and biological material, for example) and the relatively scarce security protection of them that increase extremely their attractiveness to terrorists
- The dependence of almost all the hospital processes on the informatics that can represent an important weakness on business continuity in case of malfunction/disruption
- The level of dependence of a lot of the people (patients) steadily present inside the hospital: it represents an important vulnerability in case of need to evacuate all or part of the hospital.

The physical decomposition enabled the team: to study the locations of the clinical specialties which could be a source of too many trips or of a risk dispersion, to detect unoccupied areas (missing boxes), and to define reserved roads for staff, patients and visitors. In essence, the hierarchical structure of the ‘as-is’ model and the series-parallel structure of the diagrams, allows the team to easily define a dynamic model based on flows modelling which can be extended to a horizon of several periods.

The ‘as-is’ model of OSR has been modelled using the IDEFØ method; it allows the representation of 47 units or services and 199 direct accesses between them. The critical assets of OSR have been identified and their attractiveness for terrorist attacks has been

measured through scenarios with a risk management method. The processes of critical assets have been also modelled with the IDEFØ method.

The simulation possibilities of the scenarios, thanks to the ‘as-is’ model, have been tested by modelling a flow problem and by solving the resulting linear program which includes 4,419 decision variables and 94 constraints. The computation time is around 6 seconds if we want to calculate the most crowded place, which could be the most vulnerable place of the hospital. The extension of the model for several periods (a 10 hours horizon with periods of one hour) and to several kinds of people is the next step.

The simulation of the scenarios will lead to the selection of part of or the whole model and of measured parameters. The definition of countermeasures against terrorist attacks requires the simulation of internal emergency management plans, the integration of some equipment and new practices. This will be part of the work in future Deliverable 3.2. Therefore, the specification of the ‘to-be’ model will result from the integration of equipment and best practice.

5. Recommendations

This Deliverable 3.1 has shown the efficacy of using a modelling and risk approach to the most critical assets of the hospital environment in the case of terrorist attacks. It has demonstrated how terrorist scenarios can be designed and modelled and it has studied propagation models of events by software applications using specific modelling means (i.e., IDEFØ).

This overall approach is recommended as 'best practice' or a benchmark exercise in the case of implementation countermeasures against terrorist attacks in healthcare environments. The deliverable has received input and framework reference from the previous research on healthcare risk, terrorist attack and CIP literature review and state-of-the-art from the work performed in the previous WP1 and WP2 of the Project respectively.

It is suggested that the approach could be applied as a general methodology to uncover practical and operational topics for hospitals when modelling measures to prevent or minimize terrorist events is required.

6. References:

Besombes B., E. Dubost, A. Guinet, and E. Marcon, “Médecin Traitant versus Médecin Coordonnateur ", In: GISEH 2014, 7th conference on "Gestion et Ingénierie des Systèmes Hospitaliers", Liège (Belgium), July 2014, Proceedings on CDROM, 9 pages.

Besombes B., L. Trilling, and A. Guinet, “Conduite du changement dans le cadre du regroupement des plateaux médico-techniques", Journal Européen des Systèmes Automatisés, vol. 38, 2012, pp. 689-721.

Bevilacqua M., F.E. Ciarapica, and C. Paciarotti, “Business Process Reengineering of emergency management procedures: A case study”, Safety Science, vol. 50, 2012, pp. 1368-1376.

Chabrol M., J. Chauvet, M. Gourgand, and S. Rodier, "Une méthodologie de modélisation pour les systèmes hospitaliers: Application au Nouvel Hôpital Estaing", Logistique et Management, vol. 19, 2011, pp. 3-14.

Chen W., A. Guinet, and A. Ruiz, “Modelling and simulation of a hospital evacuation before a forecasted flood”, Operations Research for Health Care, vol. 4, 2015, pp. 36-43.

DR/1/003, “Report on the threat and risk assessment of terrorist threats to the European health infrastructure”, Threats project, March 2015.

Di Martinelly C., F. Riane, J. Rappold, and A. Guinet, “Implémentation d'une armoire automatique de dispensation des médicaments dans un hôpital : une méthodologie pour évaluer la performance”, Logistique & management, vol. 19, 2011, pp. 53-68.

Doumeingts G., Y. Ducq, B. Vallespir, and S. Kleinhans, "Production management and enterprise modelling", Computers in Industry, vol.42, 2000, pp. 245-263.

Ducq Y., B. Vallespir, and G. Doumeingts, "Utilisation de la méthodologie GRAI pour la modélisation, le diagnostic et la conception d’un système hospitalier", 2nd conference on "Gestion et Ingéniérie des Systèmes Hospitaliers", Mons (Belgium), September 2004, Proceedings on CDROM, 8 pages.

Ganor B., and M. Halperin-Wernli, “Terrorist Attacks against Hospitals: Case Studies”, International Institute for Counter-Terrorism (ICT), working paper, n. 25, 2013, pp. 1-32.

Gourgand M. and P. Kellert, “An object-oriented methodology for manufacturing system modelling”, In Summer Computer Simulation Conference, Reno, Nevada (USA), 1992, pp. 1123–1128.

Guinet A., “Knowledge Acquisition and Assessment about Production Management Systems”, European Journal of Operational Research, vol. 45, 1990, pp. 265-274.

IDEF0, “Integration Definition for Function Modelling (IDEF0)”, Draft Federal Information Processing Standards Publication, http://www.idef.com/Downloads/pdf/idef0.pdf, 1993.

IMB ILOG CPLEX Optimizer, http://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/, 2015.

Kim S.H., and K.J. Jang, "Designing performance analysis and IDEFO for enterprise modelling in BPR," International Journal of Production Economics, vol. 76, 2002, pp. 121-133.

Moore D. A., “Application of the API/NPRA SVA methodology to transportation security issues”, Journal of Hazardous Materials, vol. 130, 2006, pp. 107–12.

NERC, “Identifying Critical Assets”, Critical Infrastructure Protection Committee, North American Electric Reliability Corporation version 1.0 15, September 17, 2009,

OSR Chart of Services 2014

RACAM, “Development of a Risk Assessment and Countermeasure Audit Methodology for potential terrorist attacks on mass transit systems”, CIPS European Project, http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/stories/racam_en.htm, 2011.

Ross D. T., “Structured Analysis (SA): a language for communicating ideas”, IEEE Transactions on software engineering, vol. SE-3, n. 1, 1977, pp. 16-34.

Staccini P., M. Joubert, J.F. Quaranta, D. Fieschi, and M. Fieshi, "Modelling health care processes for eliciting user requirements: a way to link a quality paradigm and clinical information system design," International Journal of Medical Informatics, vol. 64, 2001, pp. 129-142.

Vahdat K., N.J. Smith, and G. Ghodrati Amiri, “Fuzzy multicriteria for developing a risk management system in seismically prone areas”, Socio-Economic Planning Sciences, vol. 48 2014, pp. 235-248.

ANNEX 1: Suggested risk parameters rankings

Actual	Likelyhood	Suggested refinition			
Relative ranking		Relative ranking	*in years*	*per patient (in 1 year)*	
1	Very low	1	Very low	1 attack in 20 years	1 attack per 10 million patients
2	Low	2	Low	1 attack in 10 years	1 attack per 5 million patients
3	Medium	3	Medium	1 attack in 5 years	1 attack per 1 million patients
4	High	4	High	1 attack in the next 2 years	1 attack per 500000 patients
5	Very high	5	Very high	1 attack every year	1 attack per 150000 patients

Actual	Infrastructure (physical) damages	Suggested refinition			
Relative ranking		Relative ranking	*assets values*		
1	Very low	1	Very low	n/a	single day impact on infrastructure
2	Low	2	Low		Isolated impact - utilities interrupted
3	Medium	3	Medium		Multiple buildings with utilities interrupted and damage
4	High	4	High		Local area has severe damage with building disruption and utility outage
5	Very high	5	Very high		10+ structures damaged. At least two major utilities degredated by 50%+

Actual	Human Losses	Suggested refinition					
Relative ranking		Relative ranking	*n° killed*	*damage type*	*from FMEA*	*NATO CRITERIA*	
1	Very low	1	Very low	1 killed	recoverable injury in 1 week	1% people in H	No deaths of injuries or illness
2	Low	2	Low	5 killed	recoverable injury in 6 weeks	1%-5% people in H	1-5 deaths and/or 1-50 injuries or illnesses
3	Medium	3	Medium	less than 15 killed	recoverable injury in 6 months	5%10% people in H	6-25 deaths and/or 51 - 150 injuries or illnesses
4	High	4	High	less than 50 killed	non recoverable injury	30% People in H	26-150 deaths and/or 151-600 injuries or illnesses
5	Very high	5	Very high	more than 50 killed	dead (single or multiple)	>30% people in H	over 151 deaths and/or greater than 600 injuries or illnesses

Actual	Operational damages	Suggested refinition			
Relative ranking		Relative ranking	*service interruption*	*% services interrupted*	
1	Very low	1	Very low	single service interruption (1 day)	1%
2	Low	2	Low	single service interruption (days)	5% - 10%
3	Medium	3	Medium	multiple services interrpution (1 day)	10%-20%
4	High	4	High	multiple services interrpution (days)	20%40%
5	Very high	5	Very high	Most service interrption (1 or more days)	>40%

Actual	Symbolic Damage	Suggested refinition		
Relative ranking		Relative ranking	*patient confidence degrdation*	
1	Very low	1	Very low	1% reduction incoming patients (after attack)
2	Low	2	Low	2%-5% reduction incoming patients (after attack)
3	Medium	3	Medium	5%-10% reduction incoming patients (after attack)
4	High	4	High	10%-30% reduction incoming patients (after attack)
5	Very high	5	Very high	>30% reduction incoming patients (after attack)