THREATS

Terrorist attacks on Hospitals:
Risk & Emergency Assessment, Tools & Systems

Hospital's Vulnerability Assessment

Guinet Alain /Fondrevelle Julien/Chen Wanying

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

THREATS
Terrorist attacks on Hospitals:
Risk & Emergency Assessment, Tools & Systems

Outline

- **The THREATS project,**
- **The vulnerability approach,**
- **The static model of critical assets,**
- **The bridge matrix,**
- **The dynamic model for threats' propagation,**
- **The results: mitigation and response.**

THREATS Objective

To increase the resilience of EU hospitals as critical infrastructure by improving their protection capability and security awareness against terrorist attacks

THREATS Aims

- To develop a reliable method for assessing the risks and vulnerabilities of major EU health infrastructures to terrorist attacks
- To prepare specific security and threat assessment models and tools applicable to the Health sector using other EU projects
- To challenge these tools through application to the San Raffaele Hospital in Milan
- To disseminate guidelines designed to optimize the preparedness of hospitals' healthcare infrastructures against terrorist attacks

THREATS
Terrorist attacks on Hospitals:
Risk & Emergency Assessment, Tools & Systems

THREATS Partners

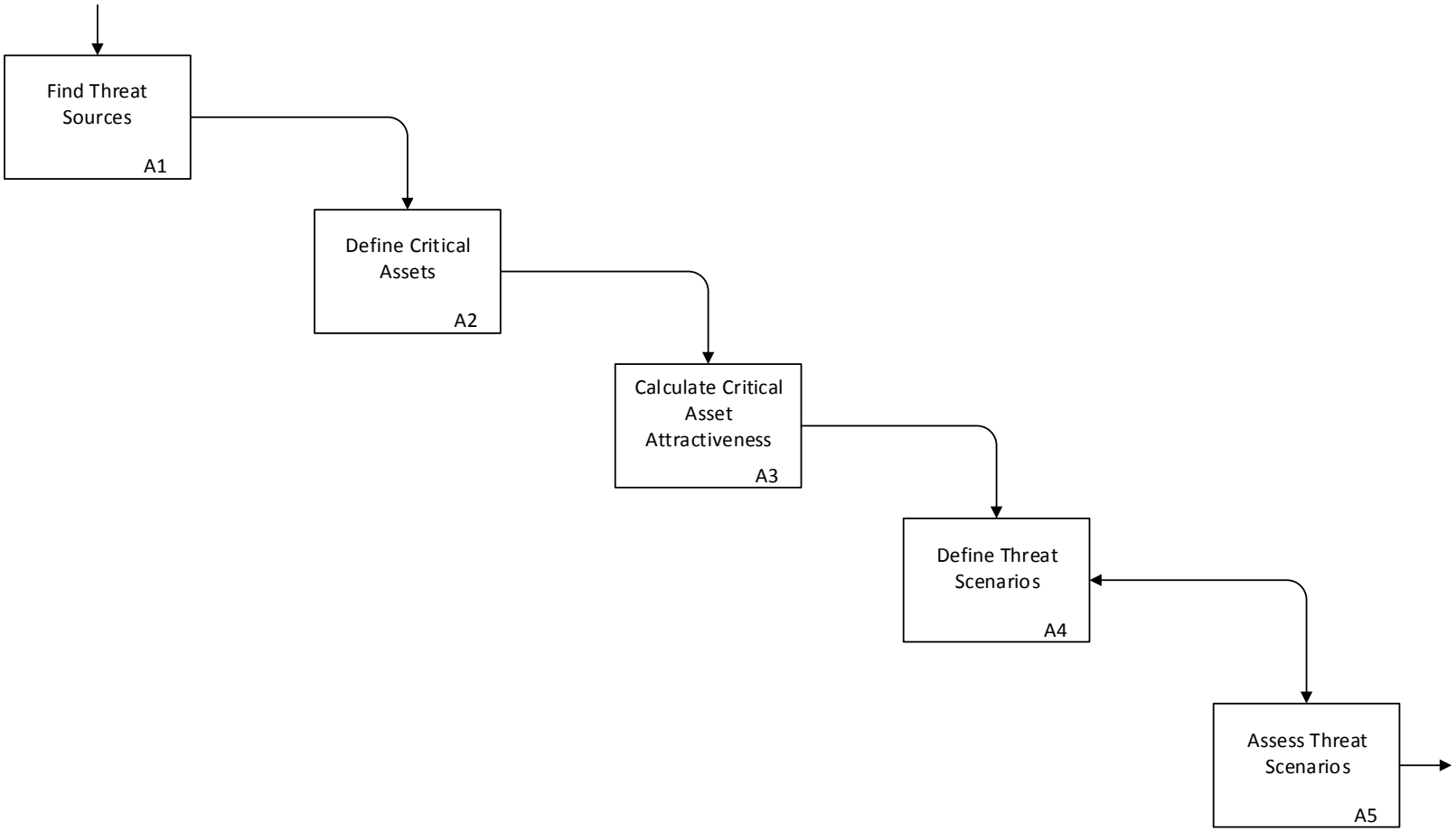
Hanover Associates (UK) Ltd®

CRIMEDIM
Centro di Ricerca Interdipartimentale in Medicina di Emergenza e dei Disastri ed Informatica applicata alla didattica ed alla pratica Medica
AMEDEO AVOGADRO
università degli studi del piemonte orientale

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

OSPEDALE SAN RAFFAELE

The vulnerability approach (1/2)

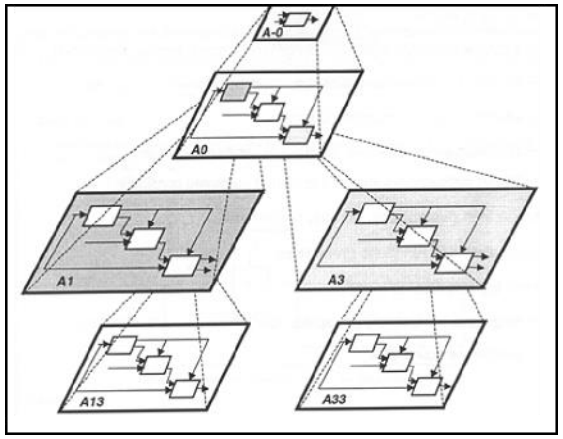


The vulnerability approach (2/2)

- Assessment of threat sources, by reviewing historical data on terrorist attacks and by analyzing their capabilities and motivations.
- Critical assets' identification, their mapping, their added-value to the hospital, their easiness of access, based on IDEF0 models.
- Attractiveness analysis based on pairing of each critical asset and of each threat source to identify potential vulnerabilities per adversary, and to approximate their likelihood.
- Scenario definition and their simulation with Linear Programming: Based on the attractiveness of the critical assets, the most likelihood scenarios with the worst consequences are constructed and investigated.

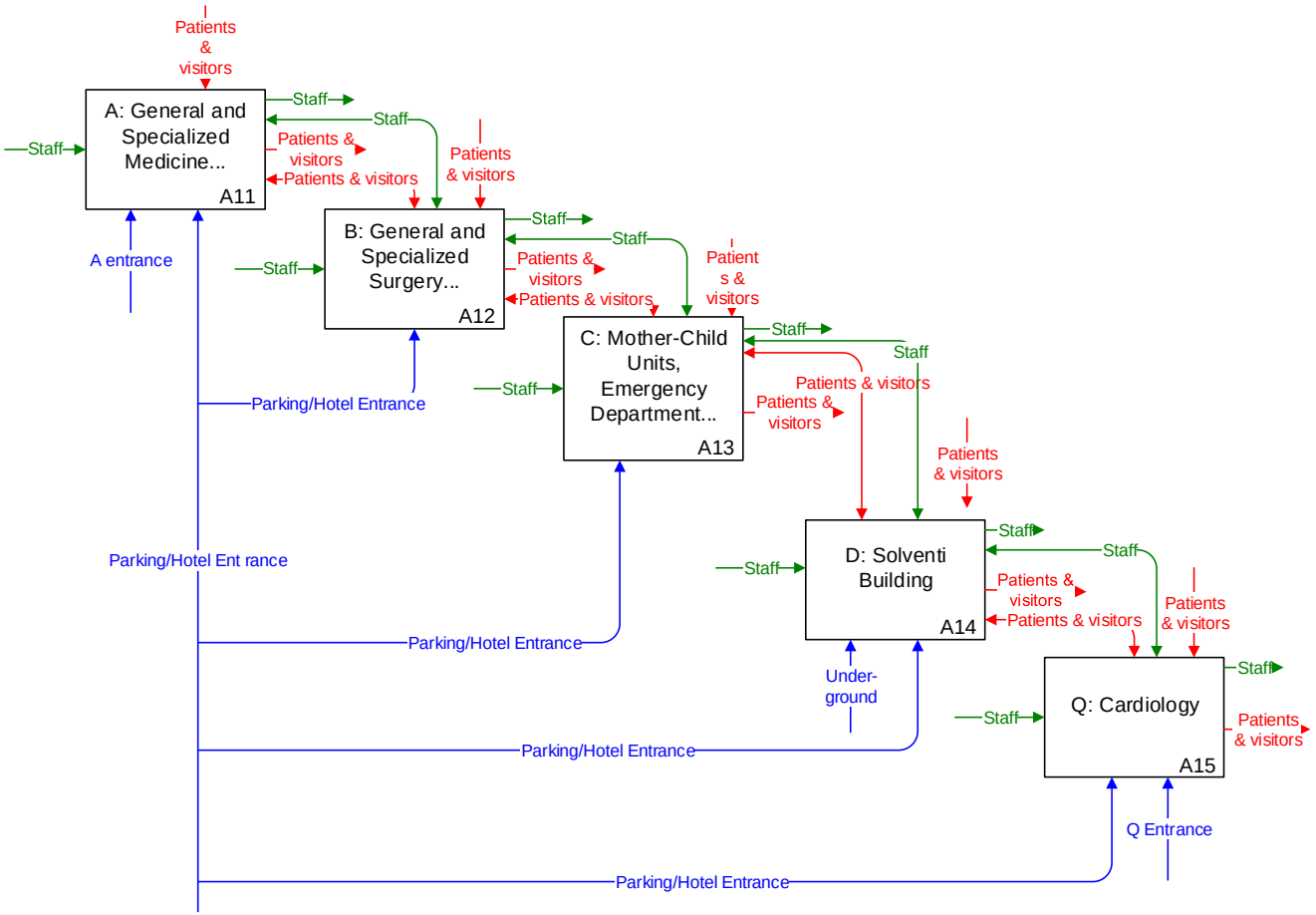
The static model of critical assets

- To represent the “AS-IS” model of OSR.
- First, a physical decomposition to model the 11 buildings, the 49 speciality clinics, the 199 accesses between buildings/levels…
- Second, a functional decomposition to model the processes of some speciality clinics which define critical assets i.e. ED, OT, ICU…
- The selection of the IDEF0 method which allows both decompositions and defines a universal language…



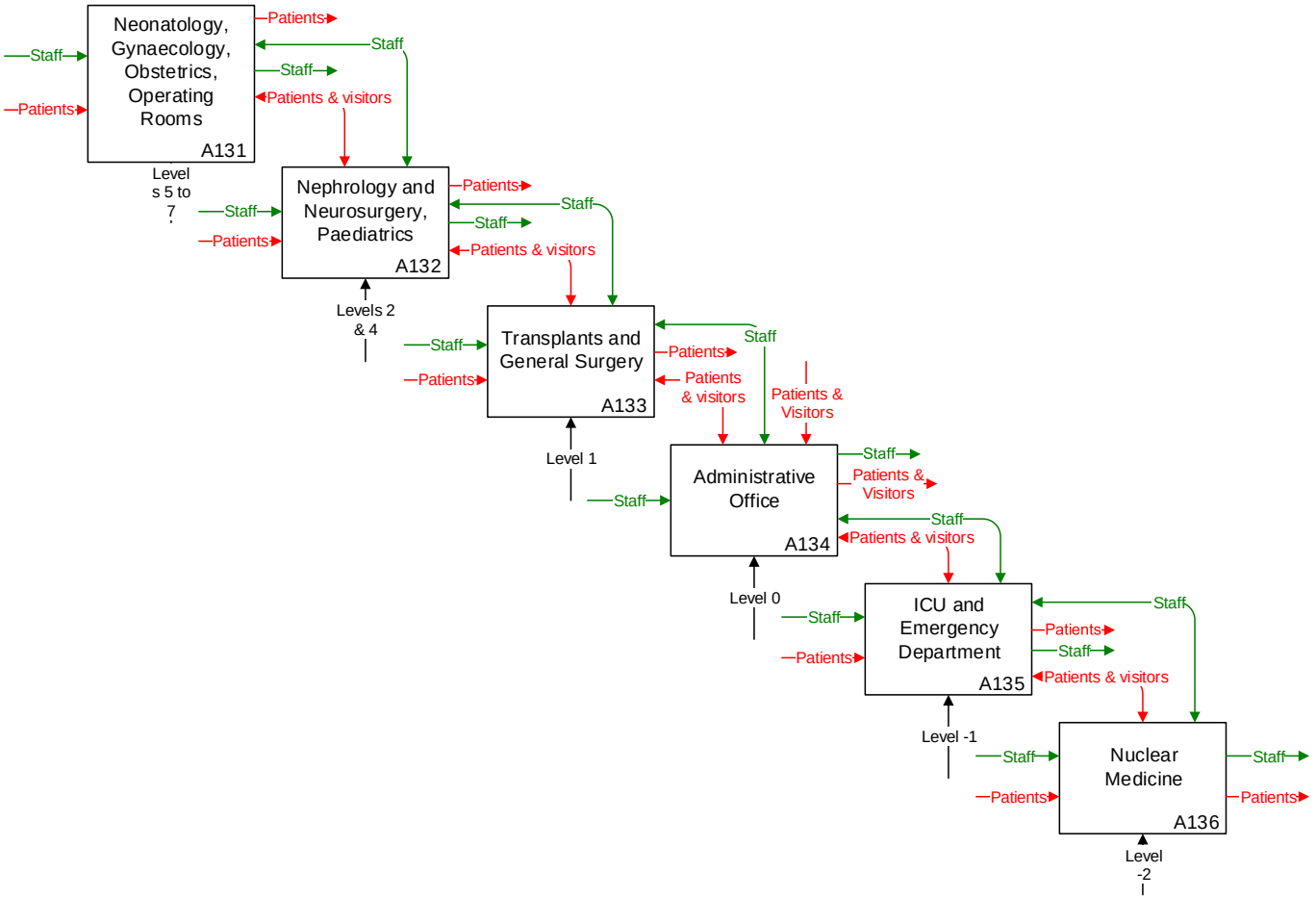
The static model: the physical decomposition

- The buildings



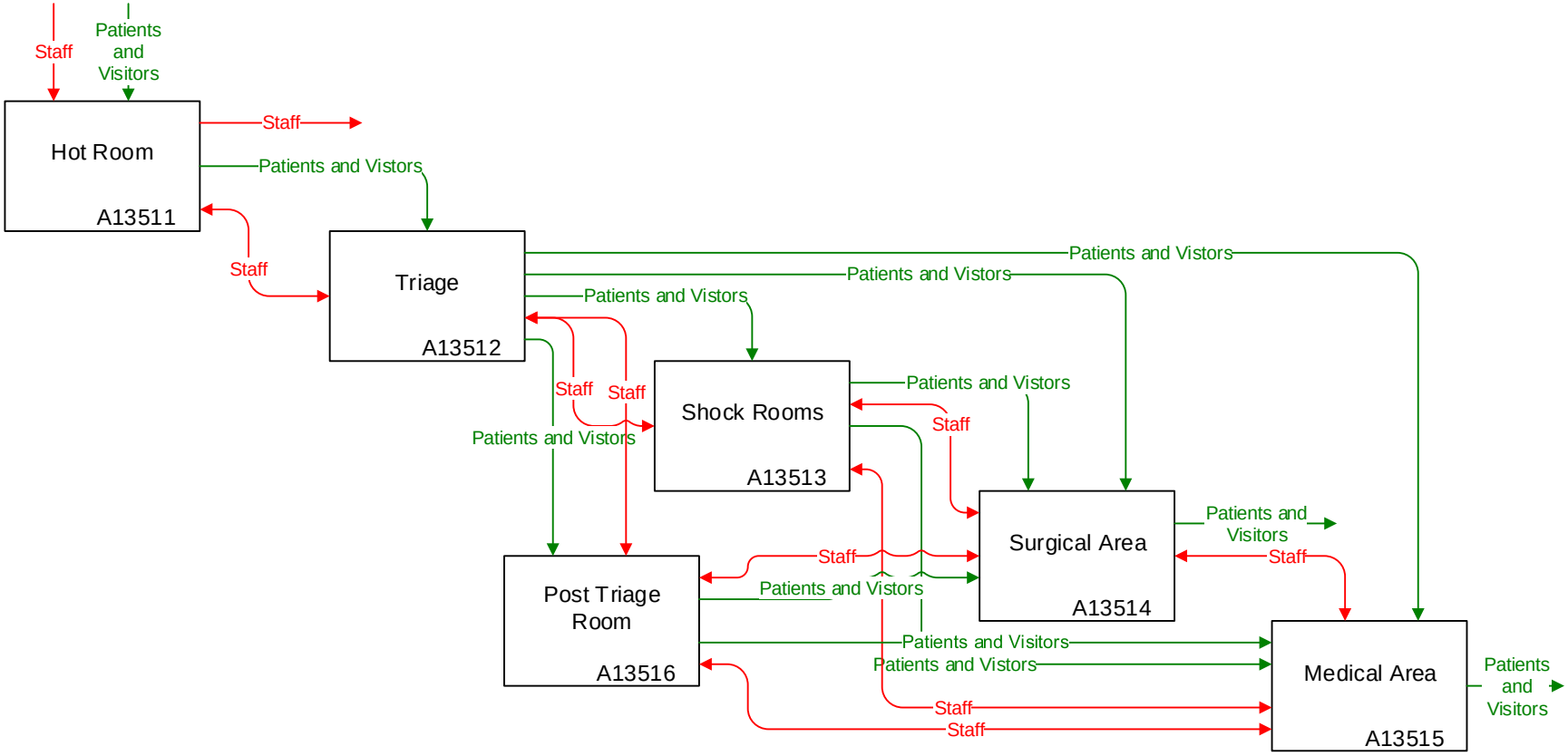
The static model: the physical decomposition

- The building levels



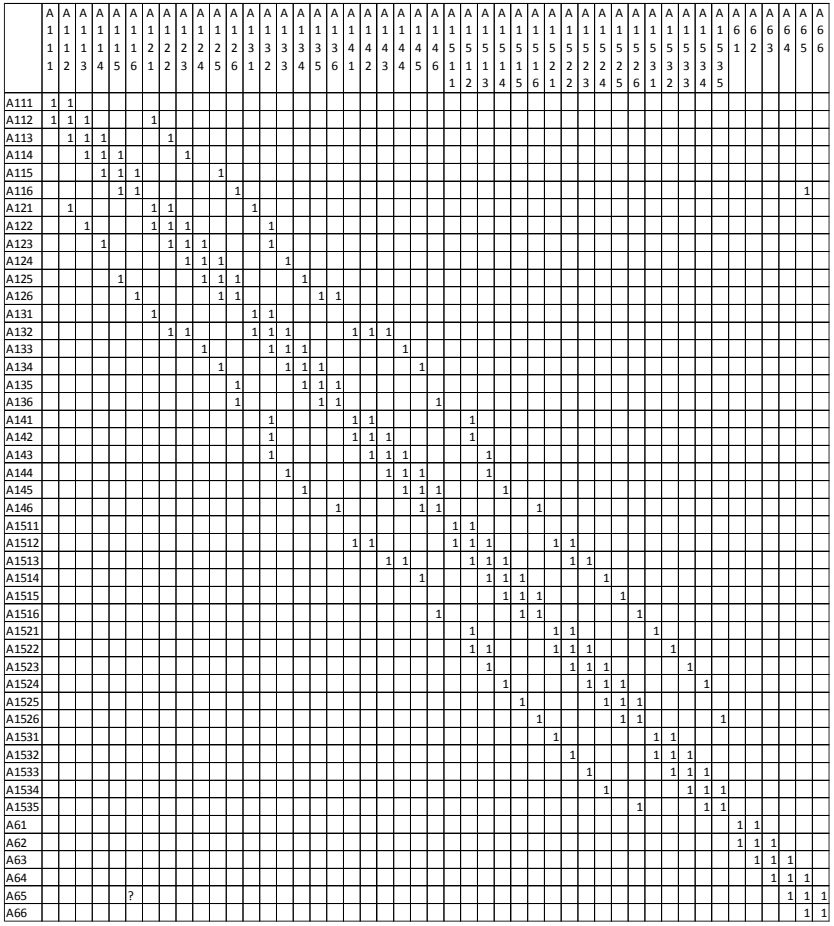
The static model: the functional decomposition

- The patient process of the Emergency Department



The bridge matrix: the accesses between care-units

- How to construct a dynamic model from the static model for flow propagation



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

The dynamic model for threats' propagation: the physical part

- The basic flow model for the care units' accesses

$$Min\ Z = \overbrace{\sum_{p=1}^{T}\left(\sum_{i=1}^{N}\sum_{j=1}^{N}\left(XG(i,j,p)+XR(i,j,p)\right)\right)*\mathrm{p}}^{Traffic} \quad (1)$$

$$\sum_{j=1|j\neq i}^{N} XG(j,i,p)*Acc(j,i) - \sum_{j=1|j\neq i}^{N} XG(i,j,p)*Acc(i,j)$$

$$+Input(i,p) \quad = \quad Inp(i,p)+Outp(i,p)$$

$$\forall i = 1,\ldots,N \quad \forall p = 1,\ldots,T \quad (2)$$

$$\sum_{j=1|j\neq i}^{N} XR(i,j,p)*Acc(i,j) - \sum_{j=1|j\neq i}^{N} XR(j,i,p)*Acc(j,i)$$

$$+Output(i,p) \quad = \quad Inp(i,p-H)+Outp(i,p-L)$$

$$\forall i = 1,\ldots,N \quad \forall p = 1,\ldots,T \quad (3)$$

The dynamic model for threats' propagation: the functional parts

- The inventory flow model, for the critical assets' activities

$$Min\ Z = \overbrace{\sum_{k=1}^{M}\sum_{p=1}^{T}(WGU(k,p))}^{Waiting\ patients} * p \quad (5)$$

$$\sum_{j=0|j\neq k}^{M} XGU(j,k,p) * Accun(j,k) - \sum_{j=1|j\neq k}^{M+1} (XGU(k,j,p+d(k)) * Accun(k,j)) + WGU(k,p) = WGU(k,p+1)$$

$$\forall k = 1,\ldots,M \quad \forall p = 1,\ldots,T-d(k) \quad (6)$$

$$\sum_{j=1|j\neq k}^{M} \left(\sum_{q=p-d(k)+1}^{p} XGU(k,j,q) * Accun(k,j) \right) \leq Capun(k,p)$$

$$\forall k = 1,\ldots,M \quad \forall p = d(k),\ldots,T \quad (7)$$

The dynamic model for threats' propagation

- A linear program has been defined based on sub-programs' integration.
- The dynamic model represents 47 care-units over an horizon of 192 periods (8 days).
- The basic flow model allows us to calculate the flow traffic in the hospital, and to define the most crowded place (i.e. the most vulnerable place for a bomb attack), or the patient contaminations, or the most isolated place, for a human aggression, or a building destruction, etc.,
- The inventory flow models enables us to simulate the patient flows in critical assets during mass casualty admissions related to external attack, or patient evacuations related to internal attack, or disrupted situations following a resource destruction, etc.

The results: mitigation and response

- Define scenarios of terrorist attacks : a facility destruction, CBRN attacks, a VIP aggression, second strike after a city attack, cyber attack, etc.,
- Calculate potential damages for the hospital with the flow model: human losses, operational damages, infrastructure damages, symbolic damages,
- Propose and simulate counter-measures for mitigation: biometric access control, video surveillance system, security guards, bacterias' sensors, etc.,
- Propose and simulate counter-measures to respond to terrorist attacks: emergency management plans, electricity generators, antibiotic stockpiles, paper kit systems, etc.

Discussion

For more information:

- Contact the THREATS Project Coordinator
  mail@hanoverassociates.co.uk
- Visit the website www.threatsproject.eu
- See our newsletter