Modelling Risk and Identifying Countermeasure in Organizations

Yudistira Asnar Paolo Giorgini

Department of Information and Communication Technology
University of Trento, Italy
{yudis.asnar,paolo.giorgini}@dit.unitn.it

1st International Workshop on
Critical Information Infrastructures Security
August 31, 2006
Samos, Greece

Trends in Software Systems

Involvement

Becoming more and more part of our life and very often they have a strong influence in our daily life decisions. Moreover, they are considered as integral and active part of the organization

Need A Methodology that .....

- Incorporate organization setting analysis and system-to-be analysis during software development process
- Anticipate uncertain event (i.e., risk) at organization level

Methodologies

SE & Org. Analysis

TROPOS and KAOS

Risk Analysis

FTA, ETA, FMECA, and HAZOP

Using software methodology as a baseline and performing risk analysis on design outcomes (even further phases outcomes)

What's Wrong

- What happens if the risk is the result of bad requirement ?
- Introducing a countermeasure can be seen as a requirement modification, is it OK ?

$$\Downarrow$$

ROLLBACK to ~~REQUIREMENT ANALYSIS~~

Hint for Modelling Framework

Doing Risk Analysis (including Countermeasure elicitation) along with Requirement Engineering Process

by

Extending Tropos in some extent by adopting NASA-DDP (Defect Detection and Prevention)

Case Study: London Ambulance Service

Having a world-class ambulance service for London staffed by well-trained, enthusiastic and proud people who are all recognised for contributing to the provision of high-quality patient care

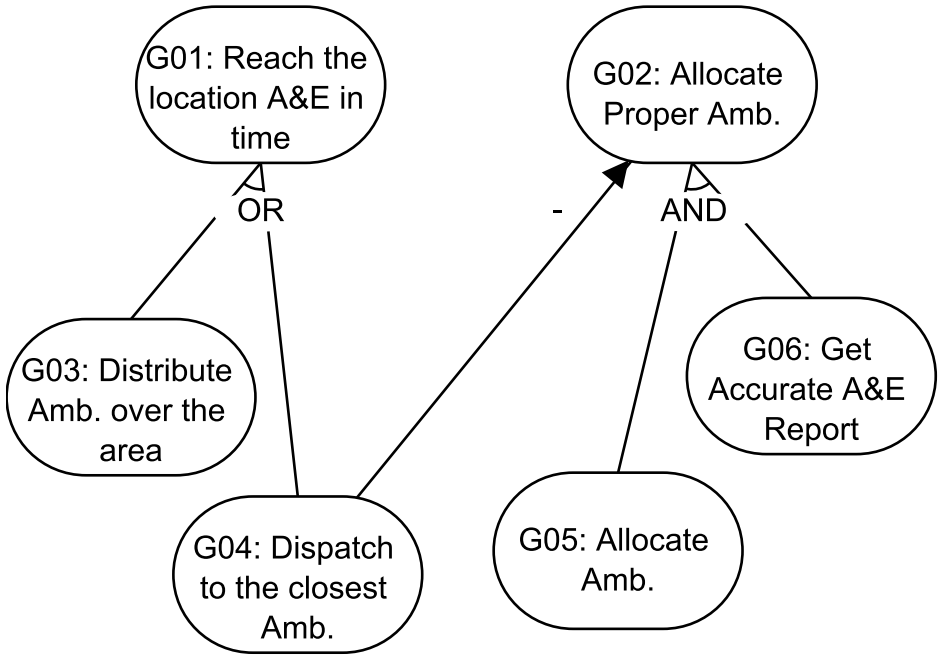
[http://www.londonambulance.nhs.uk]

Some criteria of having high-quality patient care:

- Reach the accident & emergency (A&E) location in time
- Allocate the appropriate ambulance

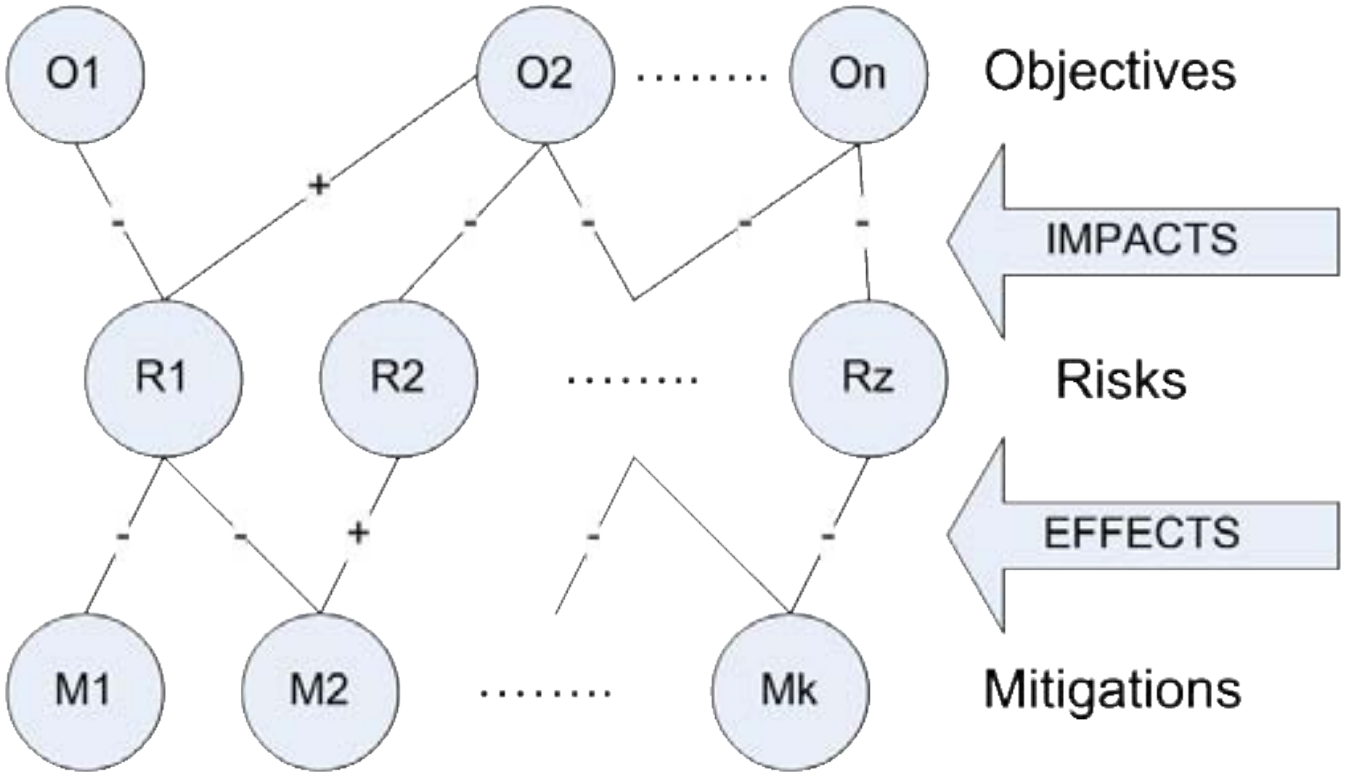
Goal Model

- Modelling strategic interest of actors in organization
- Actuator: Actor, Agent, Role, Position
- Entities: Goal, Task, Resource
- Decomposition: **OR** and **AND**
- Contribution: Positive and Negative



[Bresciani, 2004]

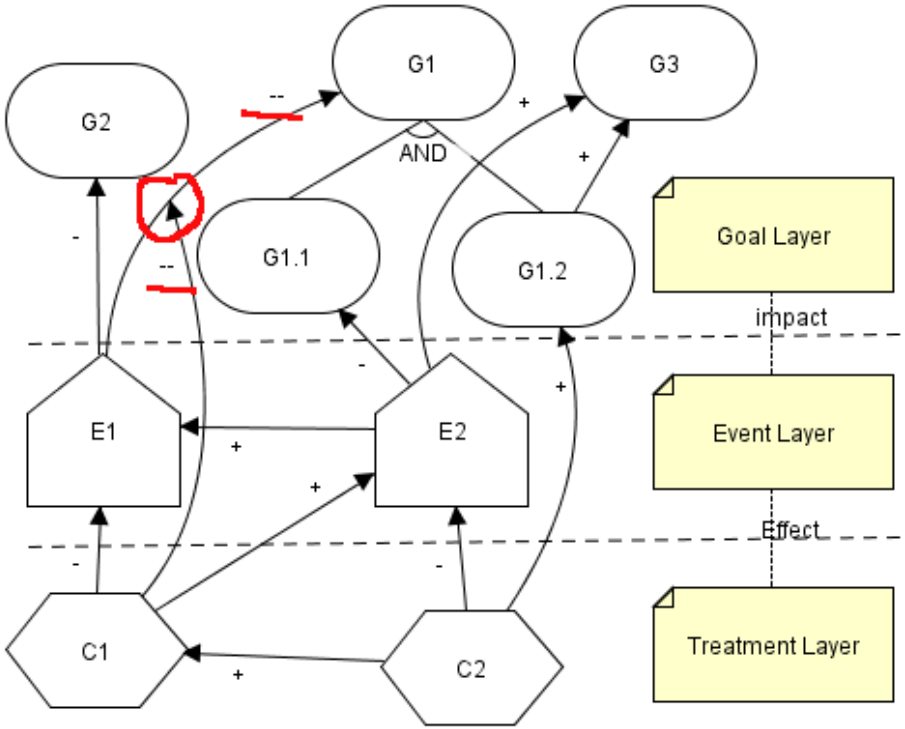
Three Layers Analysis



[Feather, 2004]

Modelling Concepts:

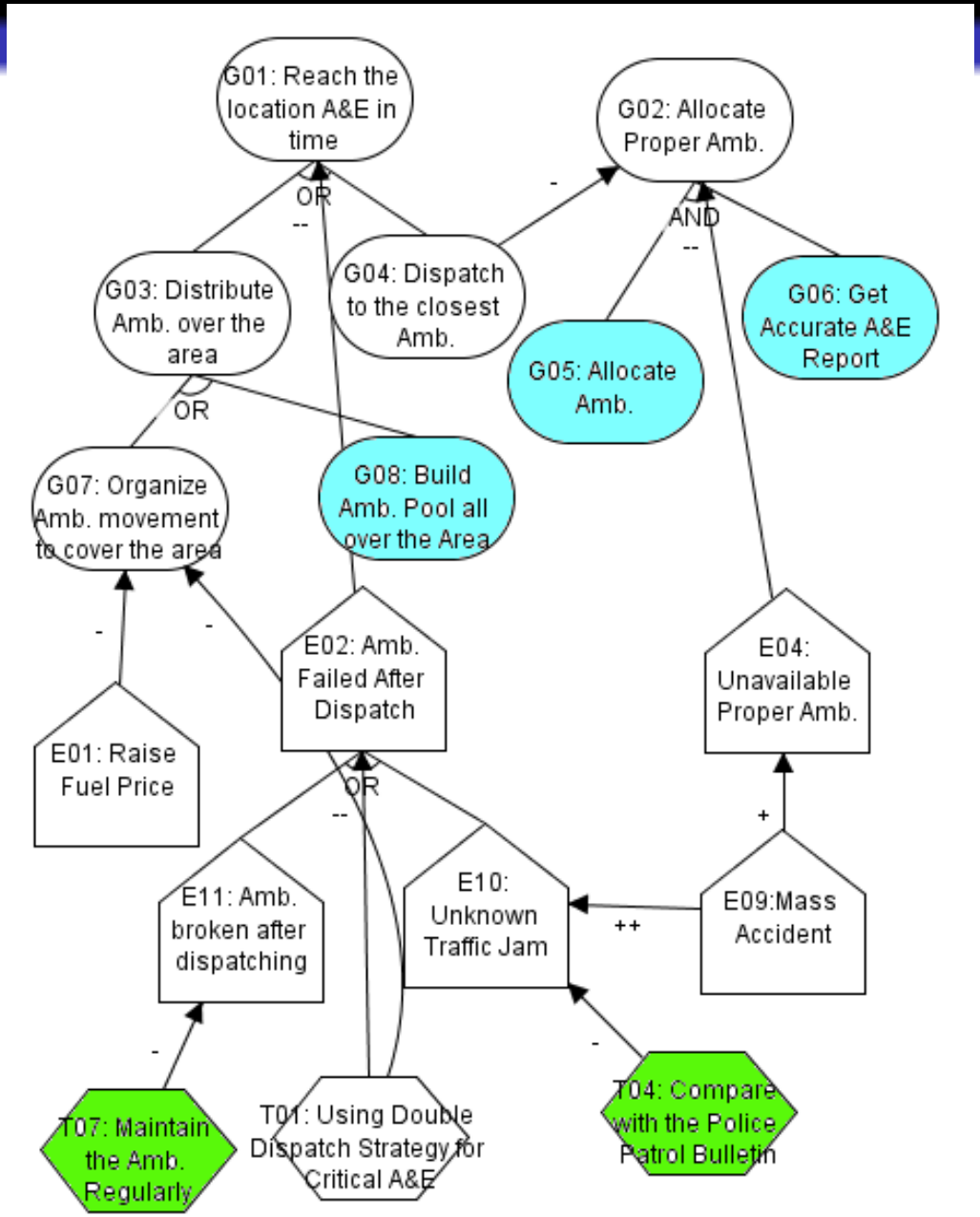
- Use Tropos Modelling Framework as much as possible
- New Concepts:
  - Extends Tropos Goal Model into three layers: Goal, Event, and Treatment
  - Modification Relation



The steps of analysis are the following:

- Find alternative solutions to satisfy the top goals
- Evaluate alternative solutions against relevant risks
- Assess countermeasures to mitigate risks

Requirements = an alternative solution + a combination of countermeasures



How we do refinement in each layer?

Goal layer

Refine the top goals into subgoals s.t. there is an actor that can fulfil it

How we do refinement in each layer?

Event layer

Define the risks of the goal layer, and refine them s.t. we can assess the risk value of the leaf.

How we do refinement in each layer?

Treatment layer

How to elicit a treatment for the event layer?

How we do refinement in each layer?

Treatment layer

How to elicit a treatment for the event layer?

Countermeasure Type

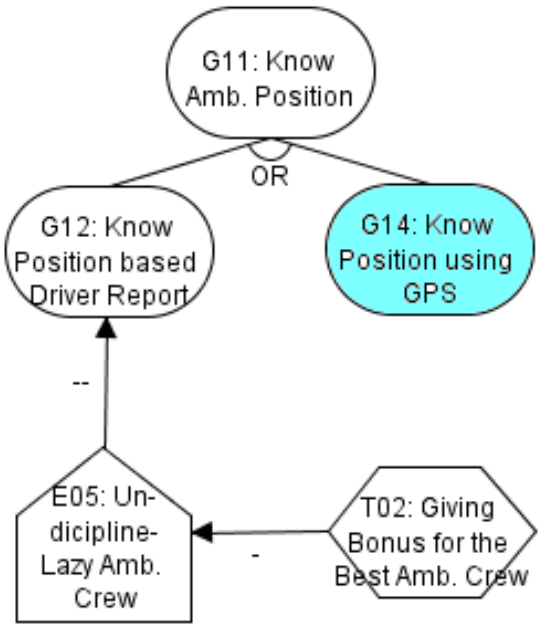
- Avoidance
- Prevention
- Alleviation
- Detection
- Retention

Avoidance

Tries to achieve the stakeholders' goals by choosing a risk free alternative

Characteristic

The goal fulfilment is very important for the stakeholder

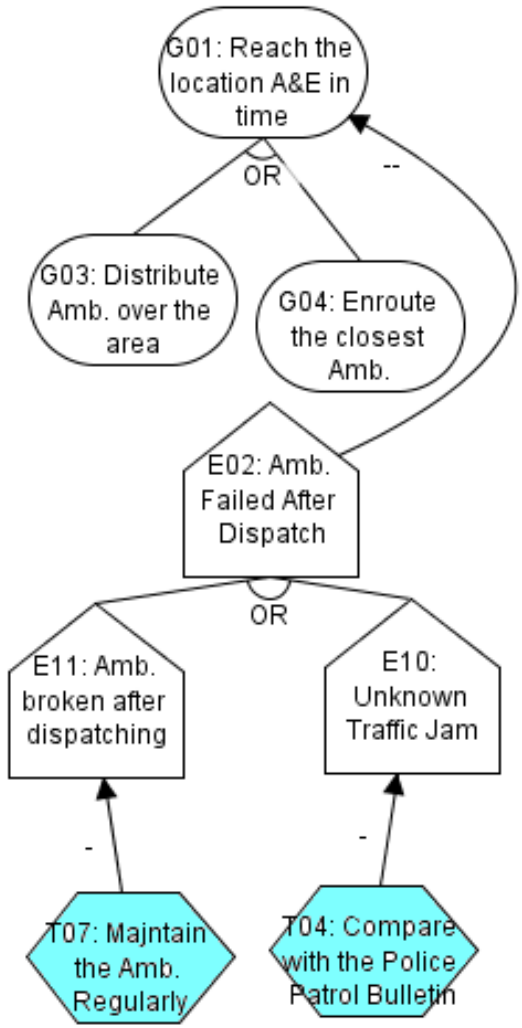


Prevention

Reduce the leaf-risks until they are acceptable for the fulfilment of stakeholders' goals

Characteristic

The risk obstructs significantly to the stakeholders' goals and it is unavoidable

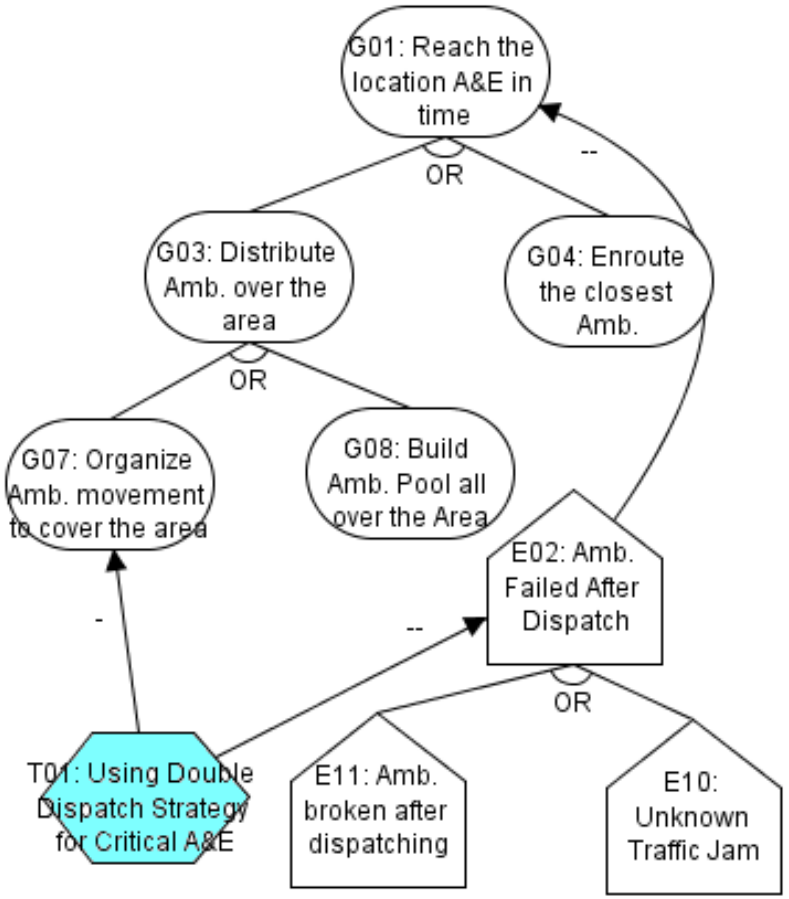


Alleviation

Reduce the risk by employing a countermeasure over the top-event

Characteristic

Can not find any measures from the previous categories

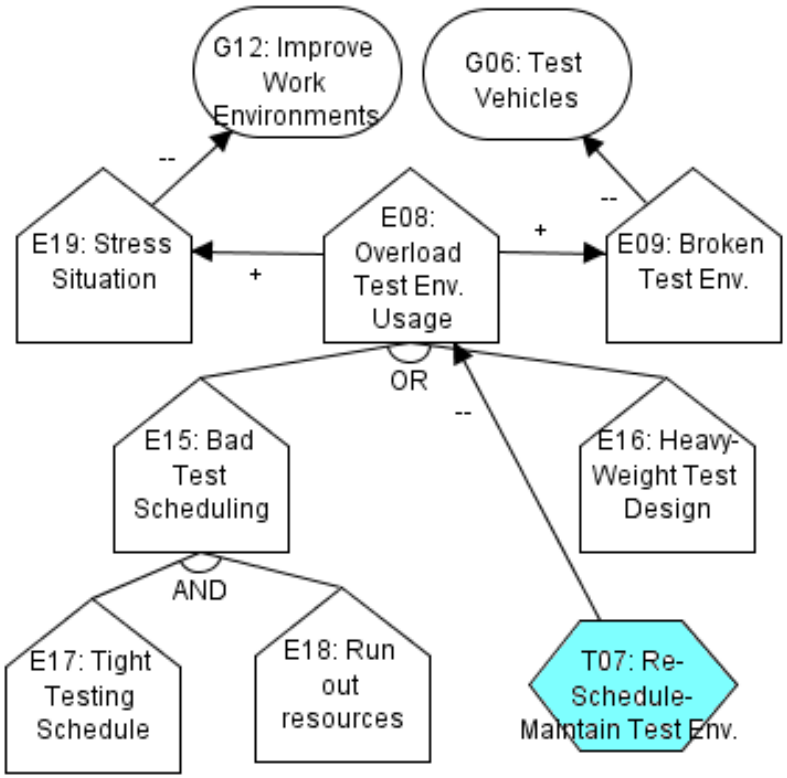


Detection

Mitigates an intermediate event in the event tree s.t it reduces the risks/top-events

Characteristic

Several top-events share an intermediate-event

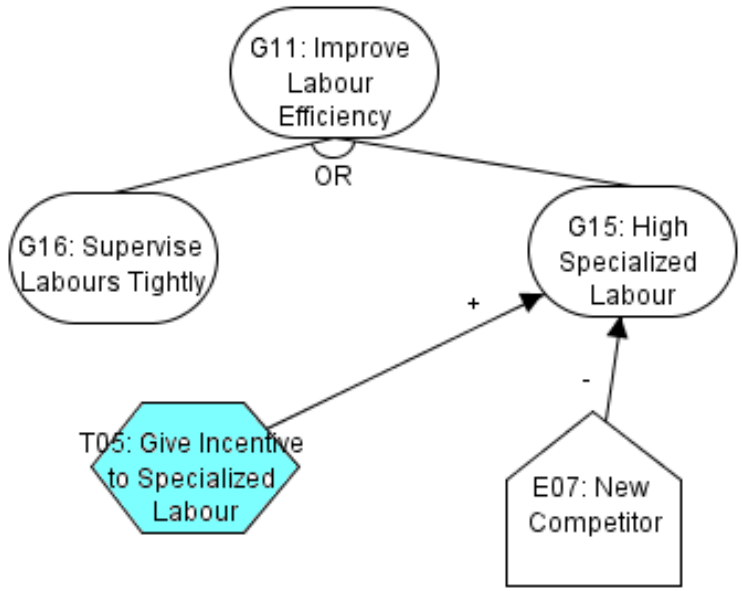


Retention

Introduce a measure that does not reduce either likelihood nor severity of the risk

Characteristic

Can not find any treatments to mitigate the risks



Achievement

- A modelling framework to analyse, evaluate, and select among the alternatives that satisfies the stakeholders' goals and satisfies the preference (e.g., acceptable risk, minimizing the total cost);
- The solution is not only based on the stakeholders' goals but it encompasses treatments to manage the impacts of malicious events;
- Categories of measure that typically are used to deal with the risks in organizations. They are categorised as: avoidance, prevention, detection, alleviation, and retention.

Future Works

Propose a quantitative reasoning mechanisms where the evidence is expressed in term of probability model

Bibliograph

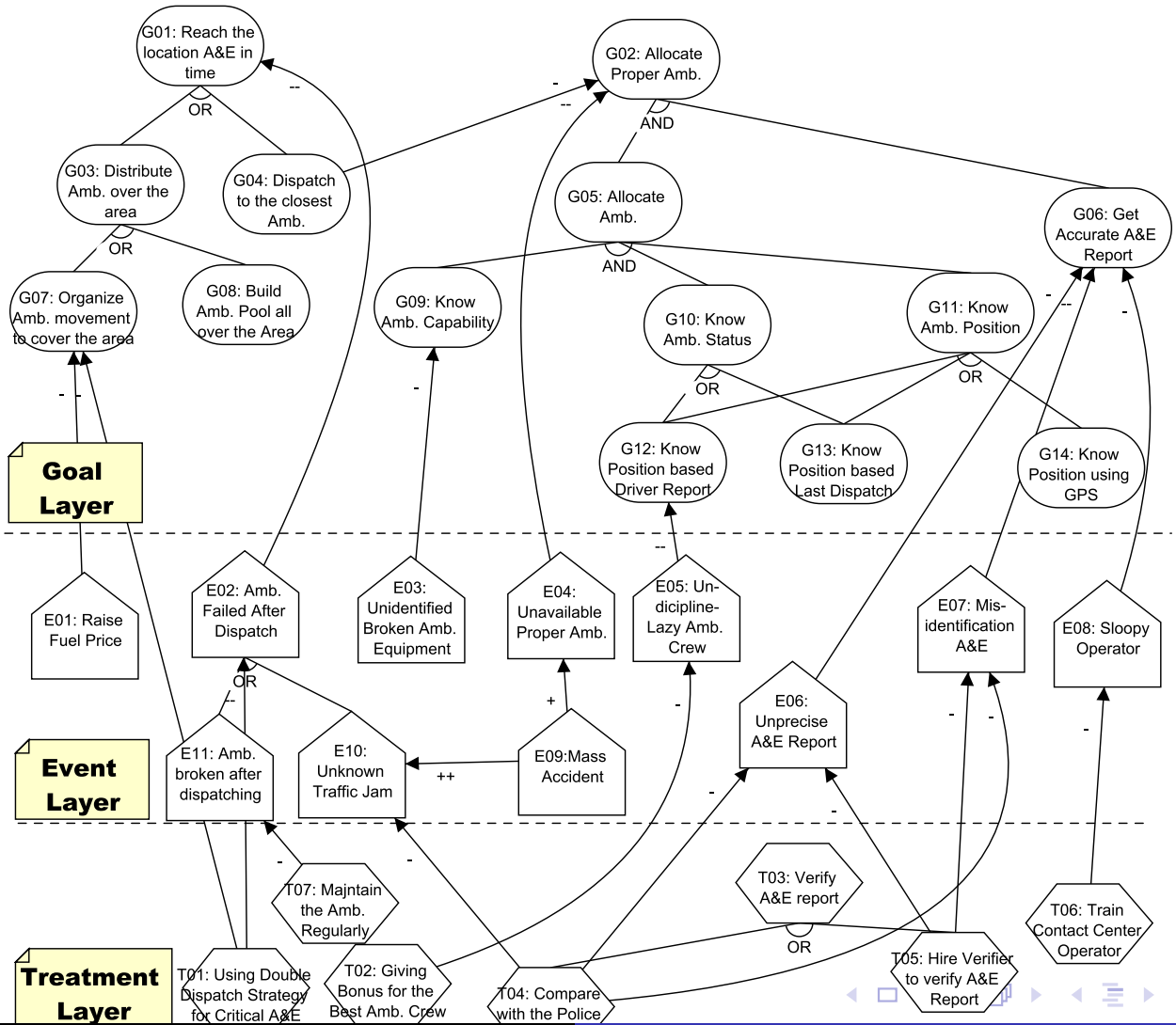
1. Asnar, Y. et. al., *Risk Modelling and Reasoning in Goal Models*, Technical Report, DIT - University of Trento, 2006
2. Giorgini, P. et. al., *Goal-Oriented Requirements Analysis and Reasoning in the Tropos Methodology*, in Journal of Engineering Applications of Artificial Intelligence, 2005, 18, 159-171
3. Feather, M.S., *Towards a Unified Approach to the Representation of, and Reasoning with, Probabilistic Risk Information about Software and its System Interface*, in 15th IEEE International Symposium on Software Reliability Engineering, IEEE Computer Society, 2004, 391-402

This work has been partially funded by SERENITY EU projects, FIRB program of MIUR under ASTRO project, and by the Provincial Authority of Trentino, through the MOSTRO project

Thank your for the attention

Discussion ?

Goal-Risk Model for LAS Case Study



GR-Tool