1 FINAL PUBLISHABLE SUMMARY REPORT

1.1 Executive Summary

The STAR-TRANS objective is to develop a comprehensive Transportation Security Risk Assessment Framework for assessing related risk and provide cohered contingency management procedures in interconnected, interdependent and heterogeneous transport networks. There are three keys aspects to this objective which make this project innovative and set it apart from other transportation security projects:

1. The first aspect relates to the approach towards transportation networks. STAR-TRANS looks at the transportation networks wholelisticly. Individual transportation networks which are very different (i.e. heterogeneous) are no longer treated in isolation i.e. rail on its own or passenger traffic flows from one mode of transportation to another, binding them together (i.e. they are interconnected and interdependent). Taken together, individual transportation networks form a "network of networks".
2. Transportation Security Risk Assessment has a renewed importance in this context. Attacks can have swelling-effects that could result in cascading failures in any asset of a "network of networks". STAR-TRANS recognizes the significant impact such situations can have and the difficulty of recognizing their existence at contingency planning stages. Risk assessment methods at the 'network of networks' level become, then, important elements of a transportation risk management process, allowing risk management teams to identify major risk contributors, the effectiveness and unintended consequences of various risk reduction options.
3. This new complex situation demands coherent contingency management procedures. The absence of which severely limits the ability to address these types of events at an operational level. This provides a basis for an integrated EU-wide approach to risk management in transportation networks that complements and adds value to the national programmes for critical infrastructure protection already in place in the Member States.

STAR-TRANS overcomes limitations in the European Programme for Critical Infrastructure Protection (EPCIP) by enhancing risk analysis and assessment through consideration of the impact that a risk incident on an asset of a transportation network may have on the assets of interconnected and interdependent transportation networks. The project outcome offers important aids to decision-makers to determine priorities among multiple contingency alternatives by evaluating the consequences, (cost, timing, resources, etc) of proposed actions. The improvement of the response and management capabilities regarding assessment of incidences / failures in critical transport infrastructures is achieved through the identification and closure of relevant knowledge gaps and through the development, validation and usage of computational modelling tools.

STAR-TRANS developed a modelling formalism which is capable of representing:possible risk incidents on European transportation networks;structure and assets of European transportation networks; dependency types between assets of interconnected and interdependent transportation networks. This formalism serves as the basis for the estimation of an incident's risk and its propagation through the "the network of networks" indicating possible unanticipated consequences.

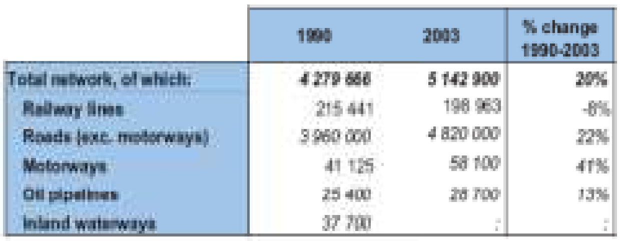
A specialised, software system (Impact Assessment Tool) was implemented that exploits the above formalism to support network operators', policy makers, insurance organizations and security professionals. The software tool provides the technology to link together any relevant assets of interconnected and interdependent transport networks. It is capable of assessing and reporting the impact that a specific risk incident on assets of a European transportation network may have on the assets of interconnected and interdependent transportation networks. Additionally, it is capable of managing European interconnected and interdependent transportation networks' structure and assets as well as dependencies between the involved assets.

1.2 Summary Description of Project Context and Objectives

STAR-TRANS objective is to develop a comprehensive Transportation Security Risk Assessment Framework for assessing related risk and provide cohered contingency management procedures in interconnected, interdependent and heterogeneous transport networks. The aim of proposed Transportation Security Risk Assessment Framework is to formalise the linkage between risk incidents, transportation network assets and dependency types between assets in order to assess the impact of an incident on the affected interconnected and interdependent networks. The proposed Transportation Security Risk Assessment Framework consists of a modelling formalism to specify transportation network structure, assets and dependencies between assets, as well as ICT-based supporting tools to generate impact assessment reports on interconnected and interdependent transportation networks in cases of risk incidents.

1.2.1 Context

There are close to 460 million citizens in the EU-25, and most of them use transport. An average of 36 kilometres is travelled every day by each citizen, and 27 of these are by car (Eurostat 2007). According to the EUROSTAT surveys (2004) an average European citizen spends about 1h12min everyday travelling by all means of transportation, which exhibits an increase of 18% in the year 2004 when compared to 1995. Car travelling continues to be the dominant transport mode (**Figure 2**). The total network size continues to grow as collectively is portrayed in **Figure 1**.



	1990	2003	% change 1990-2003
Total network, of which:	4 279 666	5 142 900	20%
Railway lines	215 441	198 963	-8%
Roads (exc. motorways)	3 960 000	4 820 000	22%
Motorways	41 125	58 100	41%
Oil pipelines	25 400	28 700	13%
Inland waterways	37 700	:	:

Figure 1. EU Transport infrastructure (Eurostat, 2007)

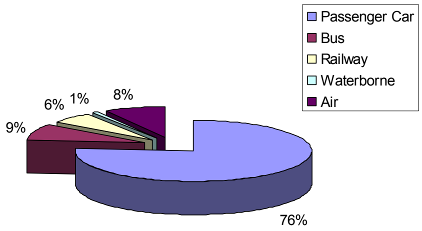


Figure 2. Passenger distribution in transport modes

When terrorists killed 191 and wounded a further 2,050 people in the coordinated attacks on the Madrid commuter rail network in March 2004, the attacks presented European lawmakers with a moment of pause and sent shockwaves through the European transport industry. At that time additional protective measures existed only in the aviation sector but Europe's mass transit systems remained wide open to attack. The London underground and bus bombings of July 2005, the alleged airline bombing plot of August 2006 and the successful airport attack of June 2007, all serve to emphasize the simple fact that answers of how best to protect Europe's transport infrastructure are much needed and long overdue.

The assets of the transportation system are precisely what make it attractive as a terrorist target. It is open and accessible, by design. It is global in its reach but institutionally diverse with many providers and operators. And it can be brutally efficient, whether moving sneakers or weapons of mass destruction. A comprehensive approach to security is needed that can meet these special challenges. It needs to be technologically sophisticated but operationally robust in harsh settings. It must be layered, not relying on any single point of interdiction. It should have "curtains of mystery," leaving the terrorist to guess as to the points and means by which passengers and cargo is screened. Finally, it must be smart and comprehensive - going beyond gates, guards, and guns, which are important elements in security but less than a total system.

Supporting these requirements strains the capabilities of existing technology, but it is a challenge that can be met.

Critical infrastructure (CI) can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour. To save the lives and property of people at risk in the EU from terrorism, natural disasters and accidents, any disruptions or manipulations of critical infrastructures should be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States (MS), their citizens and the European Union. There exist a number of transport infrastructures in the European Union, which if disrupted or destroyed, would affect two or more Member States. It may also happen that failure of a transport infrastructure in one Member State causes effects in another Member State. Such critical infrastructures with a trans-national dimension should be identified and designated as European Critical Infrastructures (ECI). This can only be done through a common procedure concerning ECI identification and the assessment of the need to improve their protection.

Figure 3. Damage of Transportation Critical Infrastructures

1.2.2 Objectives

The fundamental assumption within STAR-TRANS is that transportation assets, such as airplanes and tunnels, are integral part of larger systems. Taken together, individual transportation networks form a "network of networks". This provides a basis for an integrated EU-wide approach to risk management in transportation networks that would usefully complement and add value to the national programmes for critical infrastructure protection already in place in the Member States.

An attack on a specific asset of a transportation network must be assessed in terms of how it impacts the "network of networks" within which it resides, since it can have swelling-effects on it that could result in cascading failures. Our contribution to the risk assessment process in transportation networks is the recognition of the importance that the impact of a risk incident might have on the assets of the whole "network of networks". Qualitative and quantitative transportation risk assessment methods at the "network of networks" level become, then, important elements of a transportation risk management process, allowing risk management teams to identify major risk contributors and the effectiveness of various risk reduction options.

Specifically, STAR-TRANS overcomes limitations in the European Programme for Critical Infrastructure Protection (EPCIP) by enhancing vulnerability analysis and risk assessment through consideration of the impact that a risk incident on an asset of a transportation network may have on the assets of interconnected and interdependent transportation networks. STAR-TRANS offers important aids for decision-makers to determine priorities among multiple contingency alternatives by evaluating the consequences, (cost, timing, resources, etc) of proposed actions. The improvement of the response and management capabilities regarding assessment of incidences / failures in critical transport infrastructures are achieved through the identification and closure of relevant knowledge gaps and through the development, validation and usage of computational modelling tools.

STAR-TRANS aims at developing *a modelling formalism* in which specification of the structure and associated assets of European transportation networks as well as the specification of the dependency types between the assets of interconnected and interdependent transportation networks is facilitated. This modelling formalism considers transportation "network of networks" as consisting of assets and interdependencies which are translated to nodes and links respectively. For example, assets in a metro station might be thought of as nodes while their dependencies with assets of an interconnected rail station can be thought as links.

The determination of risks, assets and dependency types between assets are achieved through analysis of existing models and tools as well as capitalising on the experience of informal risk assessment at the "network of networks" level that took place during the implementation of the Security Program of the Athens 2004 Olympic Games and the experience from region of Bologna and the events that took place during the Bologna Massacre.

A *specialised software system* was developed to support the end users, and network operators needs. The software tool provides the technology to link together any relevant assets of interconnected and interdependent transport networks, such that risk managers, policy makers and others can, subsequently, be provided with the impact that a risk incident on an asset of a specific transportation network may have on the assets of other interconnected and interdependent transport networks. The benefits of the system are that risk managers are able to see at a glance the impact of a risk management action on the interconnected and interdependent transport network through a possible multimedia representation. Hence, risk managers, policy makers and others are able to determine alternative flows for the affected elements of transportation networks.

STAR-TRANS set up a special User Expert Group made up of transportation and security experts, to identify the research and technology resources needed to develop the proposed Risk Assessment Framework. The Group provided guidance at key points of the project. Furthermore it assisted in the assessment of the software tool developed in the projected and provided valuable feedback for their improvement.

Conclusively, the objectives of the STAR-TRANS project are:

- To produce a Security Risk Assessment Framework for European interconnected and interdependent transportation networks. The proposed Security Risk Assessment Framework includes:
    - A modelling formalism capable of representing:
        - possible risk incidents on European transportation networks.
        - structure and assets of European transportation networks.
        - dependency types between assets of transportation networks.
- A software tool capable of:
    - managing European interconnected and interdependent transportation networks' structure and assets as well as dependencies between the involved assets.
    - assessing and reporting the impact that a specific risk incident on assets of a European transportation network may have on the assets of interconnected and interdependent transportation networks.
- To evaluate the proposed Risk Assessment Framework in two specific demonstrators using the Athens and the Bologna regional transportation network, respectively.
- To disseminate the results of the project and to formulate a viable and sustainable exploitation strategy.

The project outcomes offer an integrated risk or impact assessment framework for interconnected and interdependent transport networks within the enlarged European Union. Contingency management assessment can be facilitated for the efficient command and control and the enhancement of the operational capabilities of governmental agencies, safety and security policy makers, first responders and public health authorities to unpredictable catastrophic incidents through the identification and exhaustive examination of contingency planning scenarios. Apart from better preparedness, it allows for more efficient preparedness as STAR-TRANS tools operate at the strategic level offering evaluation before expensive operations have to be used. The framework and tools facilitate communication through use of scenarios and standardization of their presentation as well as vocabulary. Thus, the project result is a reduction of the impact of risk incidents on interconnected and interdependent transportation networks that would minimize significantly social, economic and political disruptions.

In summary, the objectives of STAR-TRANS are:

- Set up a common risk assessment framework for integrated transportation systems
- Develop and validate a formal risk assessment language for integrated transportation systems
- Propose a transportation customised risk propagation model for the network assets
- Design, develop and validate the STAR-TRANS modelling language
- Design, implement, test and validate the STAR-TRANS Impact Assessment Tool (IAT)
- Apply the IAT in Bologna
- Apply the IAT in Athens
- Perform coherent dissemination of STAR-TRANS
- Develop and perform STAR-TRANS exploitation activities

1.3 Description of the Main Scientific and Technological Results/Foregrounds

The failure of one infrastructure component can result in the disruption of other infrastructures, which can cause severe economic disruption and loss of life or failure of services which impede public health and well-being. The major power blackout on August 14, 2003 lasted up to 4 days in various parts of the eastern USA, caused traffic congestion and affected many other critical infrastructures. The estimated direct costs were between $4 billion and $10 billion.

Taking containers as an example, the fact that a container could move by truck (factory to rail), rail (railhead to port), and then ship (port to port) means that vulnerabilities within one sector can be used to create an impact in another sector. Initiatives in supply chain security and supply chain management are currently addressing this challenge.

With that in mind, the objective of the STAR-TRANS project is to develop a comprehensive Transportation Security Risk Assessment Framework in order to assess transport-related risks and consequently formulate coherent contingency management procedures to be applied on interconnected, interdependent and heterogeneous transport networks.

This framework is comprised of a Risk Analysis Framework (RAF), modelling languages and supporting ICT tools for managing transportation networks, assessing and reporting incident impact. The RAF and supporting tools were evaluated for their usability, intuitiveness and market potential. They present the main scientific and technological results to come out of STAR-TRANS.

For the consortium to achieve its main results, a number of steps were taken which produced intermediate results. Before building the ICT tools, the Risk Analysis Framework (RAF) had to be created. This initiated a critical review of existing vulnerability and risk assessment frameworks published in the literature. This produced a glossary of commonly used terms in order to facilitate communication and a transportation network asset typology. The STAR-TRANS Risk

Analysis Framework (RAF) was based on the asset typology in order to formulate the proposed analysis methodology. The RAF is a fundamental outcome of STAR-TRANS as all further results reference it. User needs and demands were solicited and recorded for IAT based on the RAF. Using these requirements as a guide, the project developed two modelling languages –i.e. Impact Assessment Modelling Language (IAML) and STAR-TRANS modelling Language (STML) in order to produce formal risk assessment models which incorporated algorithms for indentifying propagated risk. This is an important moment in the project informal modelling of risk transitions to formal modeling. The user requirements and STML form integral part of the conceptual architecture for IAT. Further refinement of the conceptual architecture produced the detailed design which served as the blueprint for the implementation of IAT. IAT supports users utilising the RAF by automating portion of it. It is the tangible incarnation of RAF. After, partners decided on how they would demonstrate IAT and collect feedback on its performance from external users, they prepared and held events and proceeded to evaluate RAF and IAT. Evaluation results are a main scientific development of STAR-TRANS. It records user evaluation and acceptance of the project's outcomes.

In the following sections, the RAD, STML, IAT and evaluation are presented to the interested reader.

1.3.1 Risk anaslysis Framework

1.3.1.1 Introduction

The Transportation Security Risk Assessment Framework presented in this section formalizes the principles describing the connections between risk incidents, transportation network assets and dependency types between assets in order to effectively assess the impact of a risk incident on an asset and its effect on each interconnected and/or interdependent network.

The STAR-TRANS risk analysis framework developed in this deliverable incorporates methodological tools and approaches most extensively researched by Y. Y. Haimes and his collaborators. Tools like the Hierarchical Holographic Model (HHM) are mainly used for the identification of security scenarios and their respective associated risk. The extended RFRM (Risk Filtering, Ranking and Management) methodology offers additional relevant tools.

Asset interdependencies are modeled with a novel methodology specifically developed for STAR-TRANS which enables the comprehensive exploratory analysis of any conceivable threat scenario based on individual risk incidents together with an impact assessment on interconnected assets.

The development and the underlying approach to the risk assessment framework are the main outcomes of this deliverable.

The Risk Assessment Methodology involves the following main tasks:

1) **Security Risk inventory**. An inventory of all conceivable risk incidents within the project scope is presented, based on the systematic identification of all plausible malicious events occurring on each transport mode. The security risk inventory is drawn up based on the Hierarchical Holographic Model through the extensive examination of all possible risks.

2) **Criticality assessment**. Network assets and their dependency types are identified and the possible consequences are determined. The criticality is assessed based on the judged level of risk, defined as the combination of likelihood and consequence of risk. The cornerstone of the criticality assessment is the risk matrix which is the main tool for assessing the overall risk an incident poses based on its combination of likelihood and consequences.

3) **Description of critical scenarios**. Based on the criticality assessment, critical scenarios are described in more detail. In each scenario, the relevant transportation activity is described, using a possible sequence of events and the consequences defined in terms of fatalities and casualties, expected time out of service and economic costs. After the security risk inventory has been consolidated, it can act as a pool from which risk incidents can be

selected to be combined into any conceivable critical scenario to allow examination and exploration.

4) **Contingency planning**. Possible contingency planning operations can be defined and assigned to scenarios as appropriate. After each scenario assessment contingency plans can be produced to counter the risks simulated by the STAR-TRANS ICT tool. The framework can also be used to explore the consequences of different mitigations (contingency plans), to ensure that they have the desired effects – and avoid undesirable consequences.

5) **Response planning**. Following the materialization of threat appropriate actions must be taken. These are identified, categorized and prioritized according to the level of threat. Upon conclusion of the contingency planning, response procedure plans are constructed to formulate a general response policy framework in order to effectively reduce the inherent overall risk of the operator.

1.3.1.2 General Framework

This section defines a generalized and common RAF for interconnected and heterogeneous transportation networks based on a repetitive process of risk evaluation and severity assessment taking into account the Likelihood of occurrence and the Consequences based on certain criteria as illustrated in the diagram below:

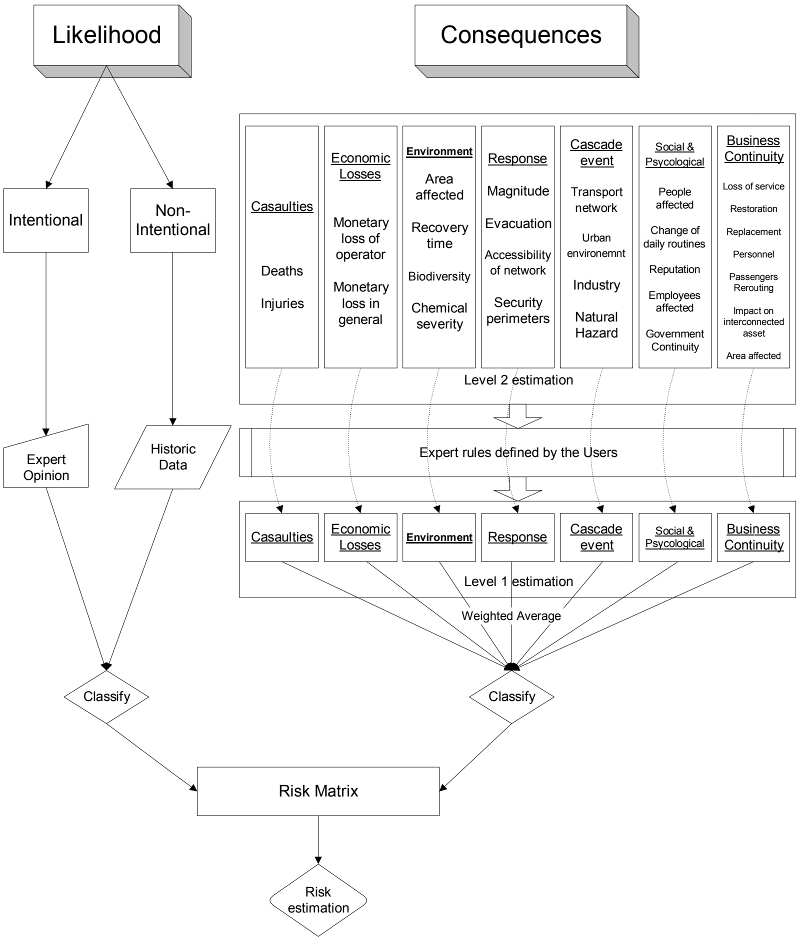


Figure 4: General Risk Assessment Framework Methodology

The definitions of likelihood and consequences are put forth:

Likelihood is the frequency of occurrence of a particular threat. In a more generic approach it is expressed by the formula

Likelihood = Intention to harm X Capability to succeed

In this approach Likelihood is directly related to the carrier of the threat as well as the vulnerability of the target.

The levels of Likelihood, in the framework, are defined according to the five level internationally accepted scale:

VERY LOW	LOW	MEDIUM	HIGH	CERTAINTY

Consequences are the result of the realization of a threat and can comprise physical harm, injury, death, loss, damage to property or revenue as well as loss in reputation and credibility of the company and of the transport system in general. More specifically, as internationally defined in the framework of the European Union, harm or damage from a possible or realized emergency/threat can be measured in the following qualitative and quantitative consequences:

- **Range:** relative to the radius of the geographic area likely to be affected by the loss or non-availability of the critical asset.
- **Severity:** the consequences of the malfunction/damage/destruction based on the following criteria:
    - The impact on the public (affected population and losses).
    - The financial impact (level of economic loss or/and degradation of products and services).
    - The impact on the reputation and prestige of the operator.
    - The environmental impact.
    - The social and psychological impact.
    - The cascading effects on other critical infrastructures and technologically related incidents.
    - The impact on the transportation network itself and on the interconnected networks.

The level of the Consequences, for the purpose of the STAR-TRANS risk analysis framework, has been described and classified based on the following internationally accepted five category scheme:

NEGLIBLE	SMALL	MEDIUM	HIGH	SEVERE

Finally, Risk is estimated through a five category system, in accordance with the previous classification of likelihood and consequences. The transformation is accomplished through the so called *Risk Matrix* show below.

Table 1: Risk matrix

	CONSEQUENCES				
LIKELIHOOD	**NEGLIGIBLE**	**SALL**	**MEDIUM**	**HIGH**	**SEVERE**
CERTAINTY	LOW	MEDIUM	HIGH	CRITICAL	CRITICAL
HIGH	VERY LOW	MEDIUM	MEDIUM	HIGH	CRITICAL
MEDIUM	VERY LOW	LOW	MEDIUM	MEDIUM	HIGH
LOW	VERY LOW	VERY LOW	LOW	LOW	MEDIUM
VERY LOW	VERY LOW	VERY LOW	VERY LOW	VERY LOW	LOW

To summarize, Risk constitutes the evaluated likelihood of occurrence of a threat that has been jointly estimated along with the severity of the impact of its realization.

1.3.1.3 Identification of assets

The identification of the network assets is the first step towards the development of the RAF as it builds the foundations upon which relevant methodologies are applied. Under the scope of the STAR-TRANS project, an asset is considered as the basic unit of any transportation network, and in general have the following properties:

- Assets are basic elements of any transportation network.
- Assets influence the security status of a transportation network and thus have value to the network, the operator, its business operations and continuity.
- Assets represent interconnected elements of transportation networks influencing the status of the entire "network of networks".
- An asset can consist of more detailed components, parts or systems. However the more detail we attempt to introduce in the analysis, the more we lose in terms of generalization and proceed into a vulnerability analysis of the specific asset.

Using the above definition as a starting point the following principles are layed down as guidelines to the conceptual risk analysis model.

Each network is modeled starting from its assets, i.e., objects with specific and easily recognizable roles.

To reduce the need for detailed information, each element is defined with a sufficiently high level of abstraction that permits consistent descriptions, starting from easily obtainable data which may however be generic or incomplete. The advantage of this approach is that transport network operators are able to conduct global risk analysis in a heterogeneous / interconnected transportation network in a predetermined environment, even if access to specific data from other operators are not immediately available:

- The external representation of all the elements (of the same or different networks) is to be kept as uniform as possible to ease the descriptions of the networks.
- The determination of risk within the transport network assets should depend only on internal parameters and the values explicitly exchanged with other assets.
- The approach does not impose any limitations on the behaviours that may be represented, leaving space for future users to interact with or modify the proposed approach.

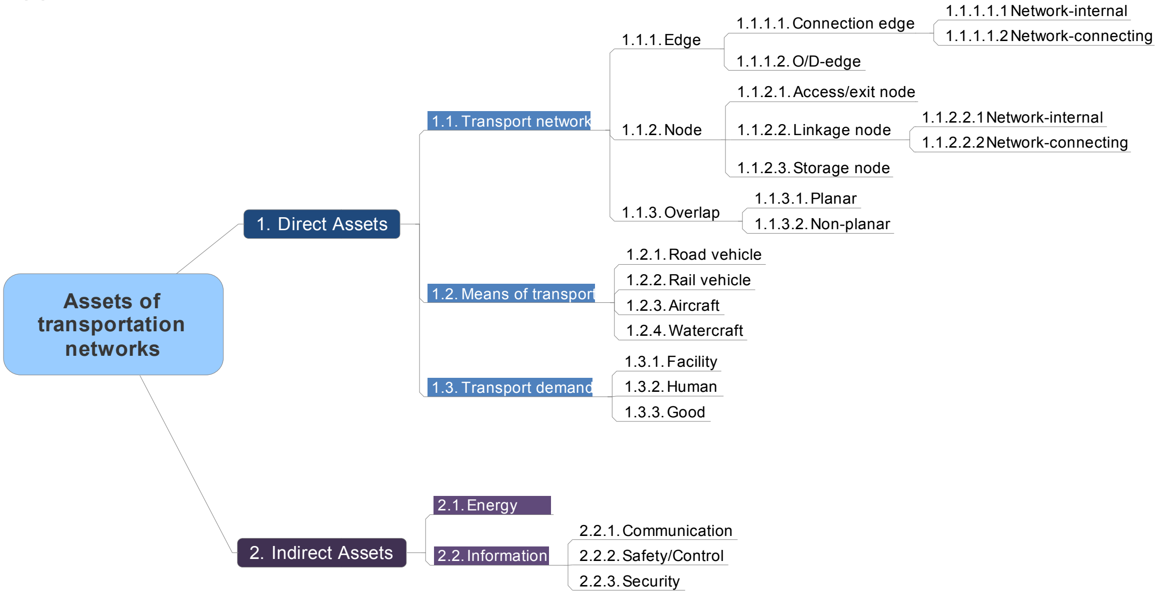


Figure 5: Hierarchical breakdown of transportation network assets

By selecting to define the assets at this level the development of the modeling procedure is facilitated while maintaining a good level of accuracy and detail for the conceptual risk analysis framework.

1.3.1.4 Identification of network / asset interconnection

The major source of complexity in heterogeneous transport systems is the way each asset affects the others as well as the intensity of that effect. In addition, assets can have self-inflicting hazards in situations where one risk incident triggers another risk incident all within the same asset e.g. an explosion causes a fire to start in the same station. This observation is used within the RAF to incorporate the notion of "self-interconnection" -the virtual relationship an asset has with itself- in order to capture secondary/evolving risk incidents within an asset. An important step in understanding and consequently modeling that relationship is to first identify all possible expressions and variations of the so-called "interdependencies" which link together assets. All interdependencies can be categorized based on the medium which each connection utilizes in order to manifest itself. These categories according to (Rinaldi, Peerenboom, 2001) are:

1. **Physical Interdependency**: Two networks / assets are physically interdependent if the state of one is dependent on the material output(s) of the other. This sort of interdependency is realized when a physical linkage between the assets exists.
2. **Systems Interdependency**: Two networks / assets have a systems interdependency, if its state depends on the properties of a system transmitted through another asset. In transportation networks these include power, signalling, SCADA, communications and IT systems.
3. **Geographic Interdependency**: Networks / assets are geographically interdependent if an incident in an asset may impact the state of assets in a defined spatial proximity. This type of interdependency is defined by the type of incident, such as explosion, fire or dispersion of chemical, biological, radiological or nuclear (CBRN) agents.
4. **Logical Interdependency**: Two networks / assets are logically interdependent if the state of each depends on the state of the other via a mechanism that does not fall into any of the above.

1.3.1.5 Threats and Incidents

A threat is any factual or probable condition (incident, fact or occurrence) that can inflict harm or death to passengers, personnel, damage or loss of transport equipment, property or/and facility as well as undermining the positive image or prestige of the operator.

A threat incident matrix was composed listing exhaustively every possible risk incident that could adversely affect the transport operator. The incidents at a transportation network asset constitute the basic building block of the RAF, where risk is calculated.

The threat identification process is based on a series of stages designed to collect information on parameters such as:

- The identification and indexing of critical infrastructures, funds and key personnel of each operator which can constitute attractive targets for individuals, groups of people or criminal organizations.
- The understanding of the present situation and the security environment within which the operator is active by taking into account the nature and type of existing criminal activity as well as hazards deriving from natural disasters and technological accidents.
- The identification and indexing of high-risk facilities, persons or other organizations and businesses which co-exist, co-operate spatially or/and are in close proximity to the Operator and are likely to be targets of criminal actions and especially terrorist attacks.

- The identification of indirect consequences as well as the capability of maintaining business continuity or fast recovery from malfunction or destruction of a neighboring high-risk target.
- The identification and indexing of sensitive access points of the Operator to other high-risk infrastructures likely to be infiltrated by individuals, groups of people or organizations.
- The identification of specific information, designs or tools held by the Operator which can be exploited by individuals, groups of people or organization to achieve their goals.

The objective acknowledgement of the above parameters establishes the identification of vulnerabilities and forms the framework for protection needs. By aiming at the impacts and consequences, instead of their causes, the design of a Security Program and management of emergencies is effective regardless of the triggering source.

1.3.1.6 STAR-TRANS Risk propagation approach

The core idea of the approach developed for modeling risk propagation in the framework of STAR-TRANS is that a user defined security scenario which originates in an asset of any transportation network can cause diverse impacts and affect other interconnected assets or networks. The entire process is described in a series of steps that are discussed in the next part of the section. Figure 5, presents an overview of the interconnected transportation network assets

It builds upon the fundamentals of Markovian chain process, so that the state of a transportation asset is dependent upon its previous state and/or the states of its interconnected assets. The state of an interconnected asset is thus a result of the nature of the incident affecting the originating asset, the characteristics of the asset under consideration (risk countermeasures, means of immediate response, etc.) and the type of interconnection between the assets.

The steps taken towards the realization of the STAR-TRANS framework are described below:

Step 1: Scenario outline definition and description of the initial incident(s) that occur(s).

First and foremost, it is important to define the initial incident(s) in terms of the nature, likelihood and possible impact as proposed in the risk analysis framework.

Step 2: Estimate Risk of the initial incident on the first Asset.

This process involves the estimation of the Risk on the first Asset, where the security incident has occurred under the examined scenario. The Risk is estimated from the Risk Matrix based on the likelihood and consequences of the incident.

Step 3: Apply the response procedures to the asset at risk

Depending on the examined scenario, procedures are applied in order to account for the optimal response to the security incident to the asset-at-risk. These include two main categories:

1. **Emergency response**. In order to account for the optimal response to the incident the following parameters must be defined: (i) the number and magnitude of responding teams, (ii) the optimal routing of the responding entities from their initial locations to the incident which may require blockage / prioritizing of roads, (iii) definition of the traffic cordon surrounding the incident area where all traffic is suspended, (iv) optimal routing to nearest hospitals for treating of injured citizens.
2. **Business Continuity**. The main target of the network operator and those closely affected by the security incident occurring at the asset at risk is to ensure the maximal possible continuation of the network operations. In order to achieve this, it is acceptable to suspend a part of the network operations or adapt to the rapidly changing conditions.

Both procedures described result in several assets of the network being considered as non-operational and a geographical interconnection established to the asset at risk.

Step 4: Determine the Assets that are interconnected to the Asset the Initial Incident occurs

The next step involves the process of identifying those Assets which are affected by the impacts of the initial incident. The new set of assets-at-risk, i.e. those linked to the first Asset by any type of linkage, is determined by (i) the type and nature of the initial incident, (ii) the type and characteristics of the interconnection between the assets. In addition to interconnected assets, secondary incidents can be triggered on the first asset as well through a **self interconnection**. To that end a separate Incident Propagation Matrix is designed for each type of interconnection (Physical/System/Geographical/Logical).

Step 5: Estimate the probability of incident initiation at interconnected assets

In the STAR-TRANS framework, this is modeled through the definition of an Incident Propagation Matrix (IPM). The Incident Propagation Matrix (IPM) is a probabilistic input / output matrix where **inputs are the** security incidents and **output(s) are also security incidents,** on the immediately interconnected asset, with the exception of geographically linked assets. It shows in a consolidated form the probability of incidents triggering in linked assets resulting from the initial security incidents.

The matrix contains either continuous probability values in the range of [0,1] or a five class likelihood values in every cell indicating the likelihood of triggering an incident in an interconnected asset (column) caused by the incident affecting the initial asset (row). These probabilities are derived from a stochastic process endowed with the Markov "memory-less" property in the sense that the possibility of subsequent incidents occurring on interconnected assets in based entirely upon the original incident and not any previous incidents preceding it.

It must be stressed that IPM *does not provide a unique "1 to 1"* mapping of incidents, in the sense that a specific incident may trigger multiple subsequent incidents.

Step 6: Estimate Risk in interconnected asset

The Risk in the interconnected / linked asset(s) is estimated using the main approach (Steps 1 and 2). However, it has to be noted that:

The likelihood of the cascading incident equals to the defined probability value of the Markovian process estimated in step 4.

Step 7: Incident termination

Subsequent incidents related to non-zero probabilities can never be brought down to zero since they are multiplied by also non-zero probabilities. This can cause an endless loop which practically serves no purpose other than overloading the system with insignificant incident occurrences. In order to alleviate this, a probability threshold is set under which the incident propagation from that incident is effectively terminated.

1.3.1.7 Incident Response procedures

The scenarios that are specified in IAT are linked to Incident Response Procedures (IRPs). Of particular interest is Scene Management. In other words, how to control and facilitate the simultaneous evacuation of citizen, routing of emergency vehicle to the scene and reroute other traffic around the area so as to enable first responders to handle the incident.

A major incident is any emergency that requires the implementation of special arrangements by one or more of the emergency services and generally includes the involvement, either directly or indirectly, of large numbers of people. They can be divided in four stages

- the initial response;
- the consolidation phase;
- the recovery phase;
- the restoration of normality.

During the initial response, scene management is organized through cordons, established around the scene for the following reasons (a) to guard the scene (b) to protect the public (c) to control sightseers (d) to prevent unauthorized interference with the investigation (d) to facilitate the operations of the emergency services and other agencies.

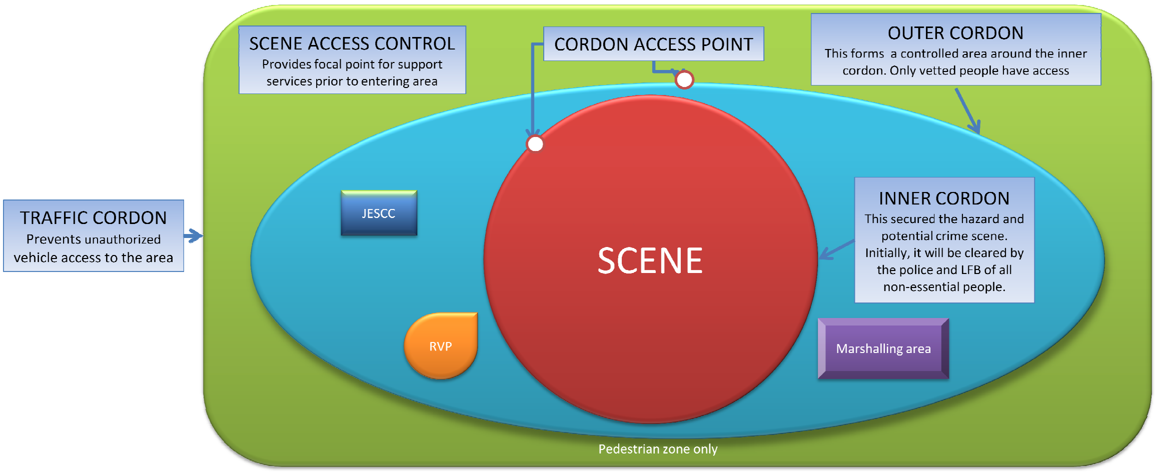

SCENE ACCESS CONTROL
Provides focal point for support services prior to entering area
CORDON ACCESS POINT
OUTER CORDON
This forms a controlled area around the inner cordon. Only vetted people have access
TRAFFIC CORDON
Prevents unauthorized vehicle access to the area
JESCC
SCENE
INNER CORDON
This secured the hazard and potential crime scene. Initially, it will be cleared by the police and LFB of all non-essential people.
RVP
Marshalling area
Pedestrian zone only

Figure 6: Scene management

The traffic cordons are established to restrict vehicle access to the area surrounding the scene. Immediate action must be taken to ensure the free passage of emergency traffic to and from the scene of the incident and to prevent congestion at and around the scene. For this reason they are of particular interest along with the specification of response action and numbers of responders.

1.3.2 STAR-TRANS Modelling Language

STAR-TRANS Modelling Language (**STML)** is a specific-purpose high-level interface language whose design philosophy emphasizes in the description of the STAR-TRANS framework. STML aims to combine language simplicity with a very clear syntax. A prerequisite for using STML is the thorough understanding of the STAR-TRANS framework’s concepts.

STML is a key element in the architectural design and implementation of the STAR-TRANS solution. It builds on Impact Assessment Modelling Language (IAML), conforming to the conceptual description of IAML, and the definition of the systemic methodology for defining a common risk assessment framework for interconnected and heterogeneous transportation systems.

As an interface language, STML provides a human or machine interface to another software component, the STML Engine Core (STEC). The STML Engine Core models all the bits and pieces of the STAR-TRANS framework, keeps the state of the whole network and tracks the risk evaluation process. STML is the command line interface for the STML Engine Core.

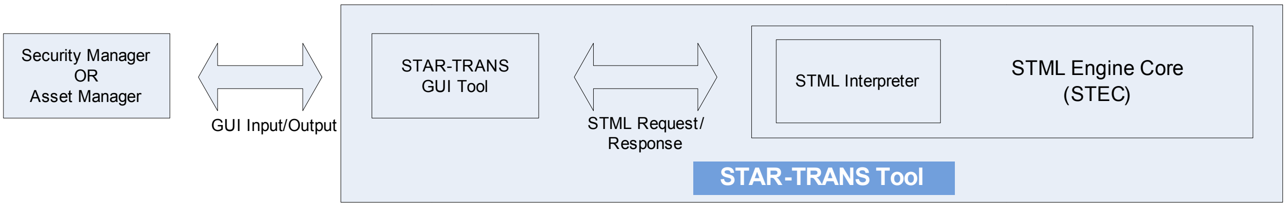


Figure 7. Graphical representation of the interaction between the end-user and the STAR-TRANS tool

Figure 7depicts the interaction between the Security Manager or the Asset Manager and the STAR-TRANS Risk Evaluation Tool. The user interacts using the STAR-TRANS user interface. The user interface formulates STML requests statements to the STML Engine Core, which modifies its internal states accordingly and returns STML responses, back to the user interface. The user interface modifies the graphical representation to the user according to the STML response it receives. The STML Engine Core combines an STML Interpreter that translates STML requests/statements into the Engine Core API and formulates STML responses based on the Engine Core return values.

STML is a modelling language, that all human interaction or machine interaction is accomplished by object **creation statements**, **set parameter statements** and **query statements**. STML is not designed to calculate risk fast and monolithically, but rather to express all the elements of the impact assessment process.

The language can be conceptually split in three different and discrete phases:

1) The definition of
   a) asset types,
   b) consequence database and
   c) threats database (define as threat-incident matrix in D1.2).
2) The description of the transportation network, describing network assets, asset's parameters and asset dependencies.
3) The recursive execution of risk evaluation and risk propagation processes.

Further, the language is designed to adhere to the following characteristics:

- **Humanly conceivable vocabulary:** The vocabulary of the language resembles spoken English. Symbols, abbreviations, and jargon are avoided.
- **Simplicity:** instructions are simple and self-explanatory. The learning curve of the language is short, even for inexperienced programmers.
- **Expandability:** The design STML is expandable, in the sense that new asset types, consequence types and threat types can be defined in the future.
- **Productivity:** STML supports all the concepts of the STAR-TRANS framework, but lacks the graphical representation that a GUI Tool provides. Using STML along with a user interface combines the flexibility and strength of STML with a graphical representation that is crucial for human understanding.

STML and the STAR-TRANS Engine Core

STML as an interface language provides an interface to the STAR-TRANS engine core that records the state of the network and the state of the risk evaluation process.

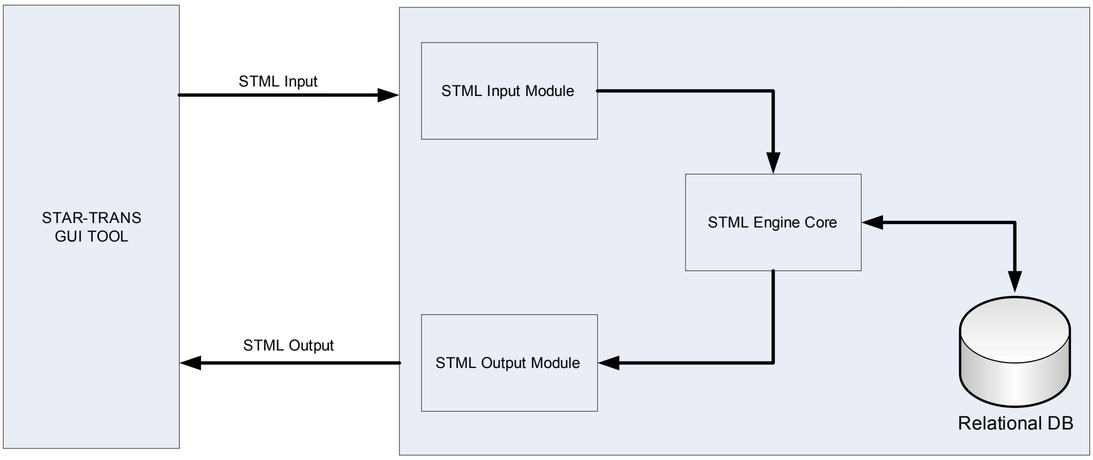


Figure 8. STAR-TRANS STML conceptual design

As shown in Figure 8 above, the GUI sends STML request statements (STML Input) upon user input. STML input module reads the STML statement and translates it into a signal suitable to the STML Engine Core API. The STML Engine Core upon reception of the input signal, checks signal validity. If validity check passes, the Engine Core consults its database, updates database information if needed and returns the appropriate STML response. A more detailed description of the aforementioned process is given in the UML 2.0 activity diagram of the STML Engine Core of Figure 9.

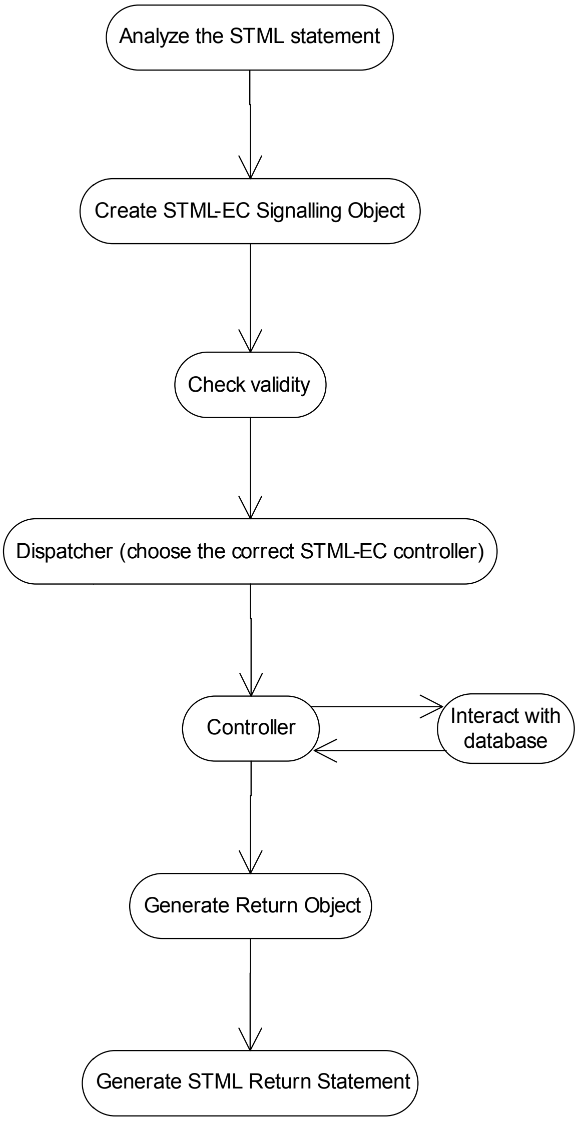

Analyze the STML statement
Create STML-EC Signalling Object
Check validity
Dispatcher (choose the correct STML-EC controller)
Controller
Interact with database
Generate Return Object
Generate STML Return Statement

Figure 9. Abbreviated UML 2.0 activity diagram that shows the processing steps of STML Engine Core for every STML input statement.

The process of every STML statement goes through can be summarized into the following processing steps:

- Analyze STML input.
- Validate STML input.
- Process validated input by the Engine Core.
- Return result.

In case a syntax or logical error is identified in any of the above steps, an error message is generated in response.

This STML engine conceptual component diagram design for the STML Engine is given in Figure 10 below:

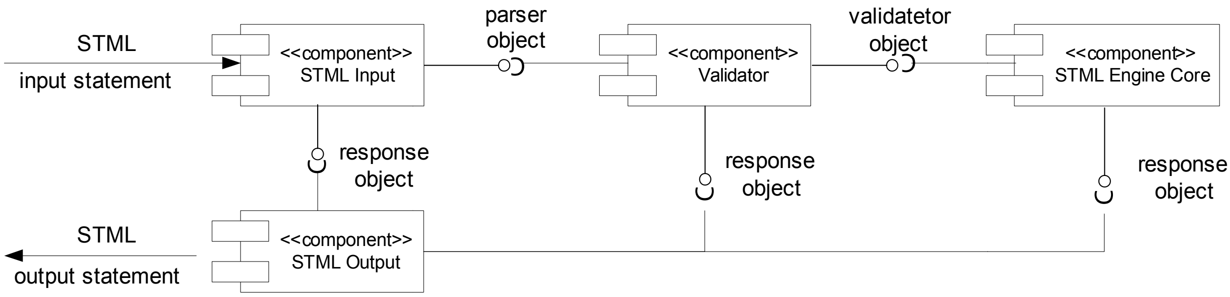


Figure 10. UML 2.0 conceptual component diagram for the STML Engine Core

The following internal components are involved in the STML Engine Core component decomposition:

1) **STML Input:** STML Input is handled to the STML Parser. It parses STML in a two level process and either generates an error object in case the syntax is incorrect or handles the result to the STML Validator.
2) **STML Validator:** The STML Validator processes the output of the STML parser and either generates an error object (in case validation does not pass) or handles its validation output to the Engine Core.
3) **Engine Core:** The Engine Core receives as input the output of the Validator. According to the different types of input the engine core can do one of the following processes:
   - Modify one of its internal databases
   - Create a new asset or delete/modify an existing asset.
   - Generate a new incident.
   - Set consequences for an existing incident.
   - Estimate propagated incidents based on initial one.
   - Response to queries related to the aforementioned areas of information.
4) **STML Output**: Receives response objects from the STML Input, the STML Validator and the Engine Core and generates the required STML response message.

Language Description

STML defines a set of abstract data types that form the blueprints of the actual data objects. Data type abstraction enhances language expandability, since the defined types can be overloaded and new types can be defined in the future to fulfil custom needs. STML supports the definition of the following abstract objects: asset types, threats and consequences database.

Asset types are the blueprints of assets. In order to create an asset its asset-type must exist. Asset types follow the categorization of the risk assessment framework. An asset-type contains the following elements:

1) Asset-type name.
2) Asset-type OID.
3) Asset-type parameters; asset-parameter definition are still pending in the STAR-TRANS project.

STAR-TRANS defines a set of asset-types. Those asset-types are contained as the standard set of assets. However, STML user can extend the current set of asset-types or even create new ones.

The risk assessment framework classifies incidents based on their respective threat source to form a five level threat hierarchy, named Threat Incident Matrix (TIM).

STML defines a consequences database, as an abstract two level consequences hierarchy. Upon the creation of a new incident, the predefined consequence hierarchy of the Consequences Database is instantiated automatically and is appended to the object of the created incident.

The STAR-TRANS framework is built on the concept of the transportation network as an integral part of a wider set of transportation networks, the "network-of-networks". STML follows this approach, by defining a hierarchical set of objects based on already defined object types. In particular STML defines the following hierarchy:

- The "network-of-networks".
- Transportation networks that belong to the "network-of-networks".
- Assets that belong to a predefined network of the "network-of-networks".

The network and the "network-of-networks" are predefined STML types, while asset types should be defined by the user.

1.3.3 Impact Assessment Tool (IAT)

The Impact Assessment Tool (IAT) can be conceptually split in three different and discrete tools which are described in more detail in the following sections:

1. The **Network Modelling Tool (NM)** that handles the representation of the transportation network, describing its assets and their interdependencies.
2. The **Risk Modelling Tool (RM)** that represents threat scenarios as networks of primary and propagated incidents and consequences on assets.
3. The **Risk Analysis Tool (RA)** that acts as a decision tool to ensure that realistic targets and commitments are established.
4. The **IAT Administration Tool (IA)** that manages the import of historical data, impact propagation matrix, threat – consequences matrix and other important data for the risk evaluation process, as well as user profiles, roles and authorization.

The IAT main requirement is the development of an intuitive interface for security experts to be able to model asset dependencies, threats and incidents, consequences, incidents' history database and the STAR-TRANS impact propagation process, to uniquely address risk assessment in the network-of-networks through risk scenarios evaluation.

IAT provides the technology to link together any relevant assets of interconnected and interdependent transport networks, such that risk managers, policy makers and others can, subsequently, be provided with the impact a risk incident has on assets of other interconnected and interdependent transport networks. The benefits of the system are that at a glance risk managers can view a graphical representation the impact of an incident response has on the interconnected and interdependent transport networks as well as determine alternative flows for the affected elements of transportation networks.

1.3.3.1 IAT Administration Tool (IA)

The IAT Administrators are equipped with intuitive graphical user interfaces to perform the following set of tasks:

- User Management
- Configure generic risk, likelihood and propagation parameters
- Import the structure of all the IAT networks represented in XML format
- Import historical data about the frequency of an incident occurrence to be used as key element for likelihood estimation

1.3.3.2 Network Modelling Tool (NM)

The Network Modelling Tool builds upon asset and network data already available in IAT through the IA Tool to formulate the integral part of the STAR-TRANS framework, the network-of-networks. The tool defines the following network hierarchy:

- The "network-of-networks".
- Transportation networks that belong to the "network-of-networks".
- Assets that belong to a predefined network of the "network-of-networks".

Users entitled with the "Asset Manager" role use predefined networks and their assets to further define networks-of-networks as an entity at the top level of the network hierarchy. The tool is "locale-aware", meaning that user and network data are organized on a geographical area basis, which allows the tool to limit the access of Asset Managers from a particular geographical area to the networks belonging to this area only.

The tool implements the following types of asset interdependencies: Physical, Systems, Geographic and Logical.

Thus the Asset Manager provides fundamental information about the structure of each network-of-networks that is a prerequisite for the STML Engine Core (STEC) in order to evaluate impact propagation and assess overall risk.

The main capabilities of the NM Tool are summarized in the following list:

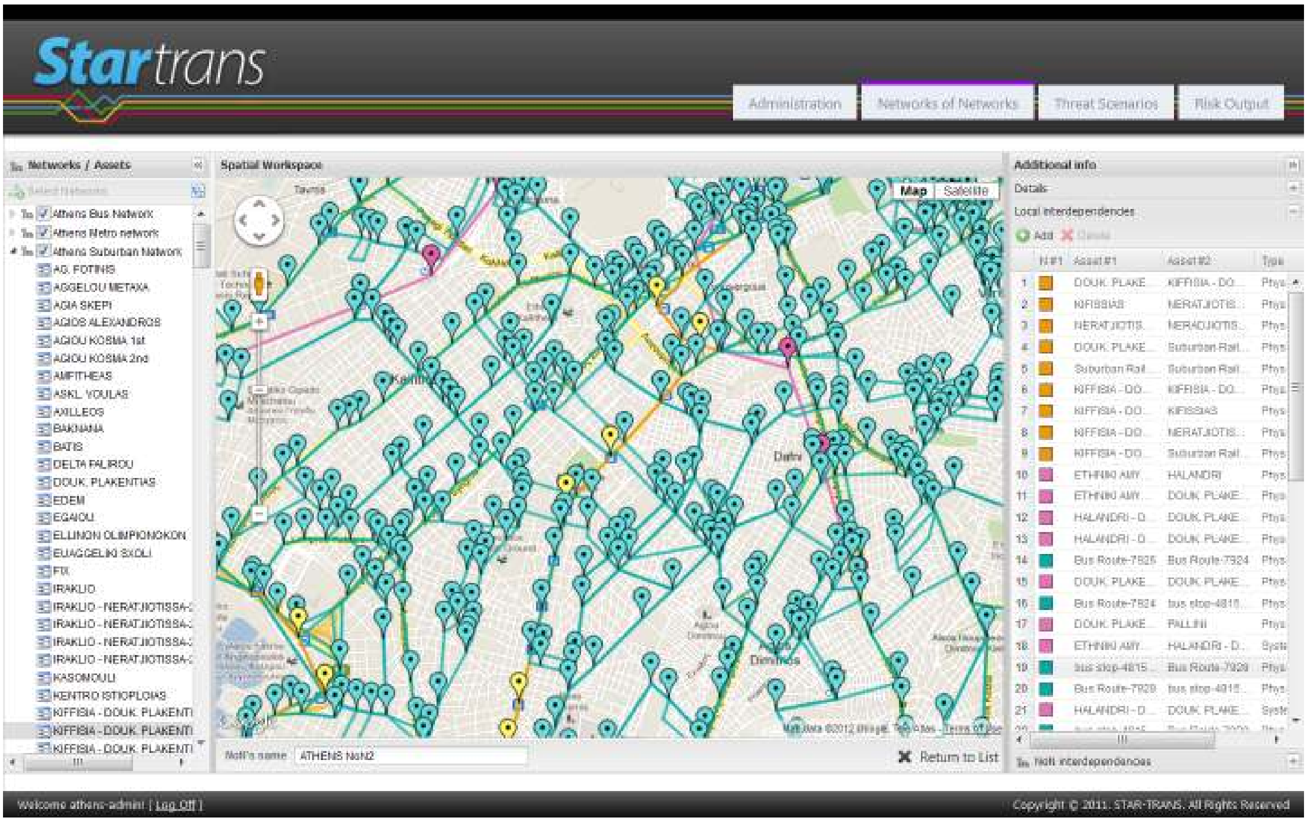
1. Advanced graphical representation of a network-of-networks using an intuitive Google Maps interface
2. Create/Read/Update/Delete operations on the asset interdependencies
3. Create/Read/Update/Delete operations on the network-of-networks level

Figure 11 depicts the Network-of-Networks Editor, which is the primary user interface of the NM Tool.

An integrated access control mechanism ensures that a network-of-networks is edited only by the user that defined it, while all other Asset Managers have the right to view or clone it to a new network-of-networks.

In the context of the NM tool a publication workflow is employed at the network-of-networks level to dissociate the network-of-networks that have been thoroughly processed and are available for public use within IAT from those that are still in draft mode and are only accessible by the user that created them.

NM relies on communication with STML Engine Core (STEC), the component of the STAR-TRANS framework that performs all modeling functions, maintains the state of the networks and evaluates risk [3]. The NM – STEC communication for network modeling are implemented with web services and ensure an integrated experience to the end user. STML Engine Core is built using the principles of Software as a Service (SaaS) and provides a standardized, well documented and thoroughly tested back-end interface to the STAR-TRANS front-end tool or any other impact assessment software. With this approach, the GUI part of any impact assessment tool is fully decoupled from the actual back-end, where the core risk evaluation process takes place.



- ☑ Athens Bus Network
- ☑ Athens Metro network
- ☑ Athens Suburban Network
  - AG. FOTINIS
  - AGGELOU METAXA
  - AGIA SKEPI
  - AGIOS ALEXANDROS
  - AGIOU KOSMA 1st
  - AGIOU KOSMA 2nd
  - AMFITHEAS
  - ASKL. VOULAS
  - AXILLEOS
  - BAKNANA
  - BATIS
  - DELTA FALIROU
  - DOUK. PLAKENTIAS
  - EDEM
  - EGAIOU
  - ELLINON OLIMPIONIKON
  - EUAGGELIKI SXOLI
  - FIX
  - IRAKLIO
  - IRAKLIO - NERATJIOTISSA-
  - IRAKLIO - NERATJIOTISSA-
  - IRAKLIO - NERATJIOTISSA-
  - IRAKLIO - NERATJIOTISSA-
  - KASOMOULI
  - KENTRO ISTIOPLOIAS
  - KIFFISIA - DOUK. PLAKENTI
  - KIFFISIA - DOUK. PLAKENTI
  - KIFFISIA - DOUK. PLAKENTI

	N#1	Asset #1	Asset #2	Type
1	🟧	DOUK. PLAKE...	KIFFISIA - DO...	Phys
2	🟧	KIFISSIAS	NERATJIOTIS...	Phys
3	🟧	NERATJIOTIS...	NERADJIOTIS...	Phys
4	🟧	DOUK. PLAKE...	Suburban Rail...	Phys
5	🟧	Suburban Rail...	Suburban Rail...	Phys
6	🟧	KIFFISIA - DO...	KIFFISIA - DO...	Phys
7	🟧	KIFFISIA - DO...	KIFISSIAS	Phys
8	🟧	KIFFISIA - DO...	NERATJIOTIS...	Phys
9	🟧	KIFFISIA - DO...	Suburban Rail...	Phys
10	🟪	ETHNIKI AMY...	HALANDRI	Phys
11	🟪	ETHNIKI AMY...	DOUK. PLAKE...	Phys
12	🟪	HALANDRI - D...	DOUK. PLAKE...	Phys
13	🟪	HALANDRI - D...	DOUK. PLAKE...	Phys
14	🟩	Bus Route-7925	Bus Route-7924	Phys
15	🟪	DOUK. PLAKE...	DOUK. PLAKE...	Phys
16	🟩	Bus Route-7924	bus stop-4815...	Phys
17	🟪	DOUK. PLAKE...	PALLINI	Phys
18	🟪	ETHNIKI AMY...	HALANDRI - D...	Syste
19	🟩	bus stop-4815...	Bus Route-7929	Phys
20	🟩	Bus Route-7929	bus stop-4815...	Phys
21	🟪	HALANDRI - D...	DOUK. PLAKE...	Syste

Figure 11: Network-of-Networks Editor

1.3.3.3 Risk Modelling Tool (RM)

The Risk Modelling Tool represents threat scenarios as networks of primary and propagated incidents and consequences on assets.

Essentially, RM is a tool for Security Managers to model long- and short-term risk using Threat Scenarios that are sets of the following primary elements:

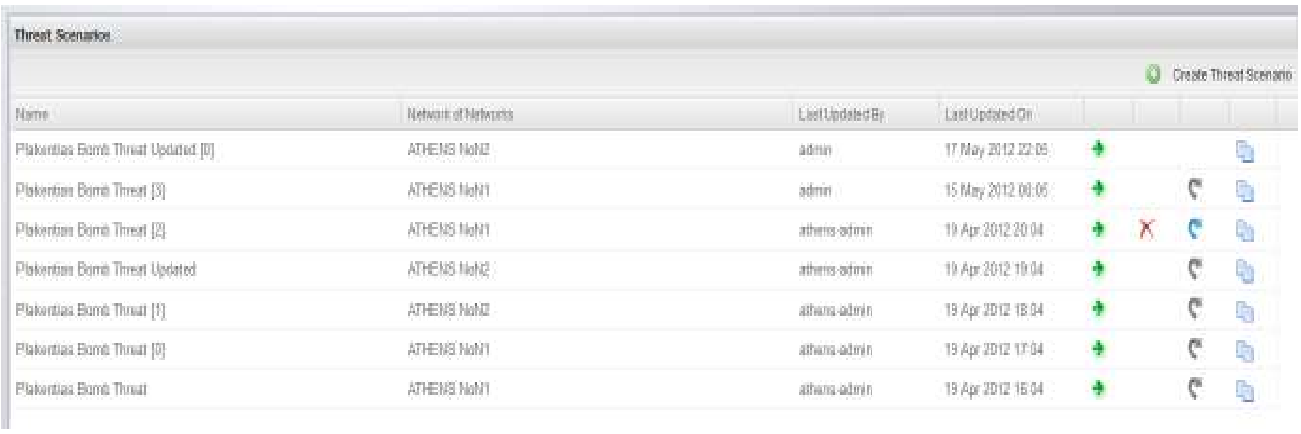
- Incident – Asset pairs that are combined to represent adverse events occurring in a particular timeframe
- Likelihood of occurrence for each Incident – Asset pair within the Threat Scenario
- Consequences of each Incident – Asset pair within the Threat Scenario
- Impact Propagation on interdependent assets

The Incident – Asset pairs of a Threat Scenario are not handled as a sequence of events on a timeline, rather as an aggregation of events that should be quantitatively analyzed typically drawing upon past experience in order to proactively manage risk.

In RM implementation the approach of a setup wizard (Threat Scenario Setup Wizard) is employed. The Security Manager is presented with a sequence of frames that lead him through a series of well-defined steps. This simplified the lengthy and complex process of fully configuring a Threat Scenario. The Security Manager is guided through the following steps:

Step 1: Create/Update Threat Scenario

The Security Manager can create a new or update existing Threat Scenario information i.e. Threat Scenario title and related network-of-networks, as shown in Figure 12.



Threat Scenarios

Name	Network of Networks	Last Updated By	Last Updated On
Plakentias Bomb Threat Updated [0]	ATHENS NoN2	admin	17 May 2012 22:05
Plakentias Bomb Threat [3]	ATHENS NoN1	admin	15 May 2012 00:05
Plakentias Bomb Threat [2]	ATHENS NoN1	athens-admin	19 Apr 2012 20:04
Plakentias Bomb Threat Updated	ATHENS NoN2	athens-admin	19 Apr 2012 19:04
Plakentias Bomb Threat [1]	ATHENS NoN2	athens-admin	19 Apr 2012 18:04
Plakentias Bomb Threat [0]	ATHENS NoN1	athens-admin	19 Apr 2012 17:04
Plakentias Bomb Threat	ATHENS NoN1	athens-admin	19 Apr 2012 16:04

Figure 12: Threat Scenario Management – Step 1

Step 2: Configure Threat Scenario

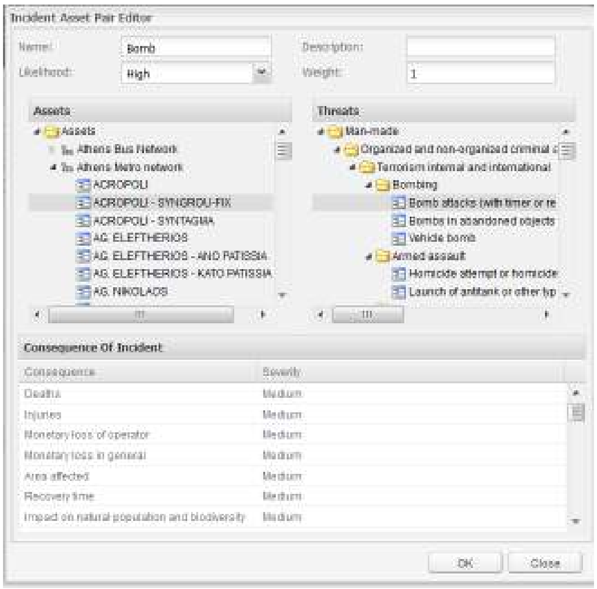
The configuration process of a Threat Scenario provides the Security Manager with the following options:

- Define Impact Propagation characteristics such as Loop, Feedback and Compounding and Impact Propagation Threshold
- Customize Threat – Consequences and Incident Propagation Matrices
- Set overall asset risk calculation algorithm
- Set algorithm to estimate risk within a Network or a Network-of-Networks from the risk values of the participating Assets

Step 3: Define Incident – Asset pairs

A new incident is categorized under the IAT threat hierarchy and characterized by an adequately detailed description. A list of networks that constitute the network-of-networks (defined in Step 1) facilitates asset filtering in order to select the asset affected by the incident.

Several Incident – Asset pairs can be thus defined before proceeding to the next step of the Threat Scenario Setup Wizard. RM only allows for unique Incident – Asset pairs. This iterative process is supported by the user interface of Figure 13.



Incident Asset Pair Editor

Name: Bomb
Description:
Likelihood: High
Weight: 1

Assets
- Assets
  - Athens Bus Network
  - Athens Metro network
    - ACROPOLI
    - ACROPOLI - SYNGROU-FIX
    - ACROPOLI - SYNTAGMA
    - AG. ELEFTHERIOS
    - AG. ELEFTHERIOS - ANO PATISSIA
    - AG. ELEFTHERIOS - KATO PATISSIA
    - AG. NIKOLAOS

Threats
- Man-made
  - Organized and non-organized criminal a
    - Terrorism internal and international
      - Bombing
        - Bomb attacks (with timer or re
        - Bombs in abandoned objects
        - Vehicle bomb
      - Armed assault
        - Homicide attempt or homicide
        - Launch of antitank or other typ

Consequence Of Incident

Consequence	Severity
Deaths	Medium
Injuries	Medium
Monetary loss of operator	Medium
Monetary loss in general	Medium
Area affected	Medium
Recovery time	Medium
Impact on natural population and biodiversity	Medium

Figure 13: Incident Asset paid definition dialogue – Step 3

Step 4: Define Likelihood of occurrence

For each Incident – Asset pair the Security Manager is requested to define the likelihood of the selected incident to occur on the related asset. Likelihood can be equivalently expressed in ordinal or cardinal scale.

Step 5: Define Incident Consequences on Asset

RM suggests a list of consequences derived from the Threat-Consequences Matrix of Step 2. According to risk assessment framework, the set of consequences are: Casualties, Economic Losses, Environment, Response, Cascade event, Social & Psychological and Business Continuity.

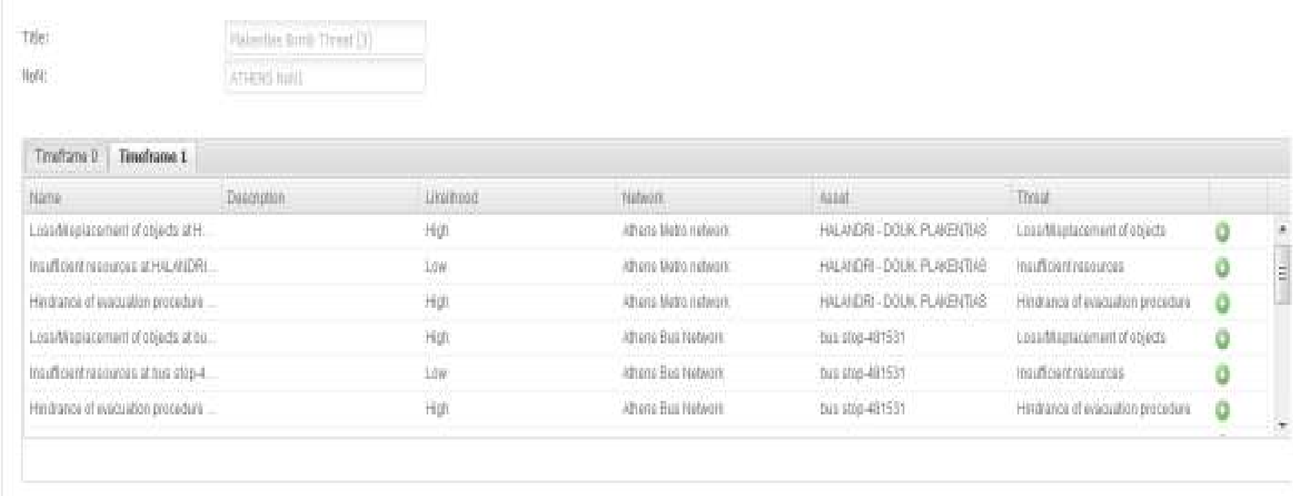
The Security Manager drawing upon past experience can eliminate certain elements of the list and/or add new consequences particular to the situation that is investigated. Each consequence is characterized in a quantifiable manner by its severity.

The Consequences dialogue in Figure 13 shows the implantation of the interface for the Security Manager to accurately select the incident consequences on the pre-defined asset.

Step 6: Define Consequences of Propagated Incidents

After a complete Threat Scenario is defined, RM evaluates the possible propagated incidents that arise from the incident-asset pairs of the scenario. For each propagated incident on a particular asset RM suggests a list of consequences derived from the Threat-Consequences Matrix and the Incident Propagation Matrix of Step 2. It is the Security Manager's responsibility to eliminate certain elements of the list and/or add new consequences particular to the situation that is investigated. Each consequence is characterized in a quantifiable manner by its severity. All propagated incidents carry the likelihood of their initiating incident.

The propagated incidents and their consequences are displayed in Figure 14, where each incident-asset pair title is originally empty.



Title: Halandri Bomb Threat (1)

RoN: ATHENS RoN1

Name	Description	Likelihood	Network	Asset	Threat
Loss/Misplacement of objects at H...		High	Athens Metro network	HALANDRI - DOUK. PLAKENTIAS	Loss/Misplacement of objects
Insufficient resources at HALANDRI...		Low	Athens Metro network	HALANDRI - DOUK. PLAKENTIAS	Insufficient resources
Hindrance of evacuation procedure ...		High	Athens Metro network	HALANDRI - DOUK. PLAKENTIAS	Hindrance of evacuation procedure
Loss/Misplacement of objects at bu...		High	Athens Bus Network	bus stop-481531	Loss/Misplacement of objects
Insufficient resources at bus stop-4...		Low	Athens Bus Network	bus stop-481531	Insufficient resources
Hindrance of evacuation procedure ...		High	Athens Bus Network	bus stop-481531	Hindrance of evacuation procedure

Figure 14: Threat Scenario Editor Wizard

In general, the RM Tool is able to interoperate with STML Engine Core (STEC) via web service calls and exchange all information necessary for STEC to perform risk modelling related processes.

1.3.3.4 Risk Analysis Tool (RA)

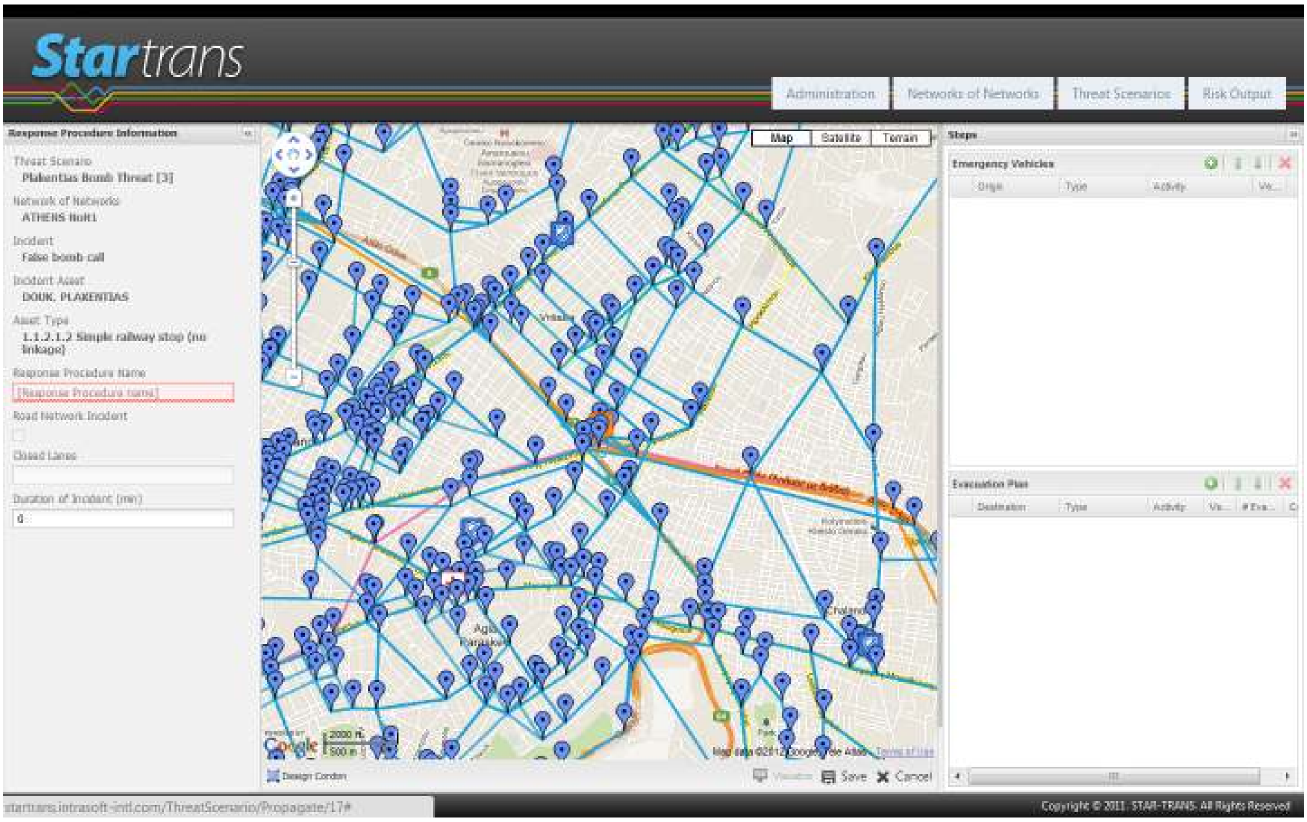
The output of Risk Analysis is a valuable decision assistance tool both to ensure that realistic targets and commitments are established, but also to make choices among alternative courses of action that offer different levels of risk and costs, savings or other consequences. Options available to the parties controlling the transportation network or network of networks can be integrated into the analysis to evaluate their overall impact on a particular course of action.

The Risk Analysis Tool comprises the following modules:

1.3.3.5 Response Procedure Module (ReP)

Each Response Procedure is associated with an Incident-Asset pair and is also linked to a network-of-networks. The Risk Analyst gains an overview of this related network-of-networks on a map, where the outer cordon of the incident scene should be interactively defined. Additionally, the Risk Analyst defines the emergency and evacuation vehicles origin and destination respectively as well as purpose. Along, with number of lane closures and incident duration, ReP communicates this information to VISTA through web service calls which calculates routing of emergency vehicles.

Figure 15 shows the ReP module user interface.



Response Procedure Information

Threat Scenario
Plakentias Bomb Threat [3]

Network of Networks
ATHENS NoN1

Incident
False bomb call

Incident Asset
DOUK. PLAKENTIAS

Asset Type
1.1.2.1.2 Simple railway stop (no linkage)

Response Procedure Name
[Response Procedure name]

Road Network Incident
□

Closed Lanes

Duration of Incident (min)
0

startrans.intrasoft-intl.com/ThreatScenario/Propagate/17#

Figure 15: Incident Response Procedure Editor

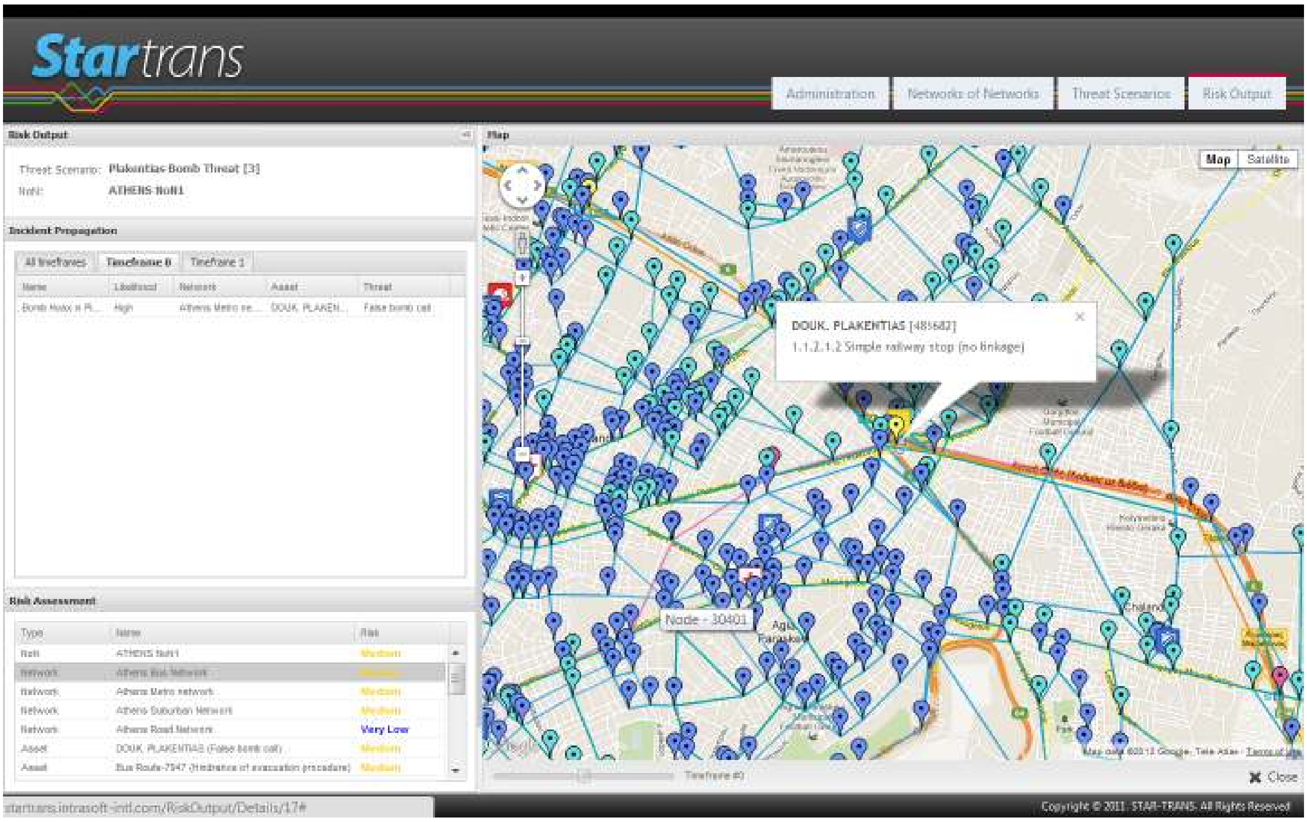
1.3.3.6 Risk Output Evaluation Module (Rout-eval)

Having estimated the impact and likelihood of each risk, the Risk Output Evaluation Module (Rout-eval) assess the overall risk contained within a network, network of networks or area of effect with respect to a specific Threat Scenario.

Rout-eval captures all parameters related to a Threat Scenario to equip Risk Analysts with a tool that offers them the following information:

- Graphical representation of the position of a selected Incident – Asset pair on a map
- Indication of the overall risk involved with this Incident – Asset pair
- List of propagated incidents
- Overview of the corresponding Response Procedure
- The overall risk of the asset involved in the pair, its corresponding network and network-of-networks.

Risk Analysts process the aforementioned information using the Risk Output Editor interface of Figure 16.



Risk Output

Threat Scenario: Plakantias Bomb Threat [3]

NoN: ATHENS NoN1

Incident Propagation

All timeframes | Timeframe 0 | Timeframe 1

Name	Likelihood	Network	Asset	Threat
Bomb Hoax in Pl...	High	Athens Metro ne...	DOUK. PLAKEN...	False bomb call

Risk Assessment

Type	Name	Risk
NoN	ATHENS NoN1	Medium
Network	Athens Bus Network	Medium
Network	Athens Metro network	Medium
Network	Athens Suburban Network	Medium
Network	Athens Road Network	Very Low
Asset	DOUK. PLAKENTIAS (False bomb call)	Medium
Asset	Bus Route-7547 (Hindrance of evacuation procedure)	Medium

DOUK. PLAKENTIAS [481682]
1.1.2.1.2 Simple railway stop (no linkage)

startrans.intrasoft-intl.com/RiskOutput/Details/17#

Copyright © 2011. STAR-TRANS. All Rights Reserved

Figure 16: Risk Output Editor

1.3.3.7 Overview of the IAT Import Format

For the purposes of the STAR-TRANS project, the following data ingestion process has been proposed. The underlying concept is described in Figure 17.

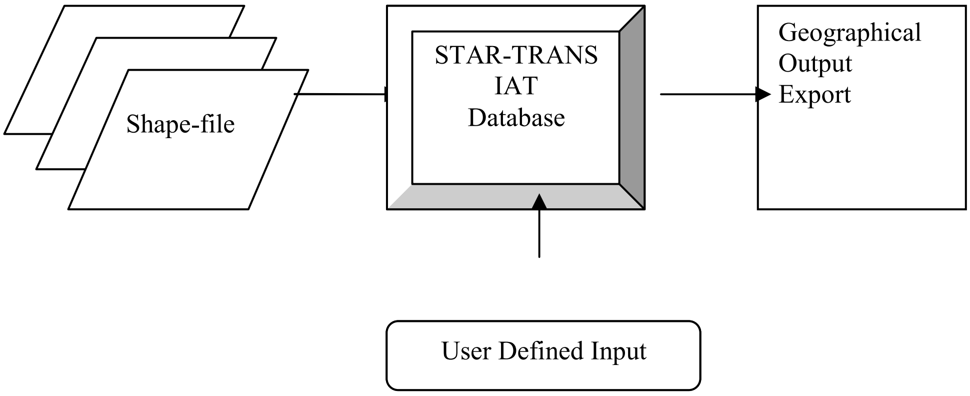


Figure 17: IAT data ingestion process

The IAT user may feed the system with two distinctive processes:

1. Provide existing geo-referenced datasets in a common format
2. User defined information, selecting from a menu displaying existing information (e.g. network assets and attributes)

The input data are introduced as files each one containing a number of assets (and their characteristics) that has to be matched with the elements of the database of the IAT tool. The user are provided with matching screens to pair characteristics of the input files (elements of the database) to the asset characteristics that are utilized by the IAT. The input files should be in GIS Shape Files format.

1.3.3.8 Interfacing to VISTA

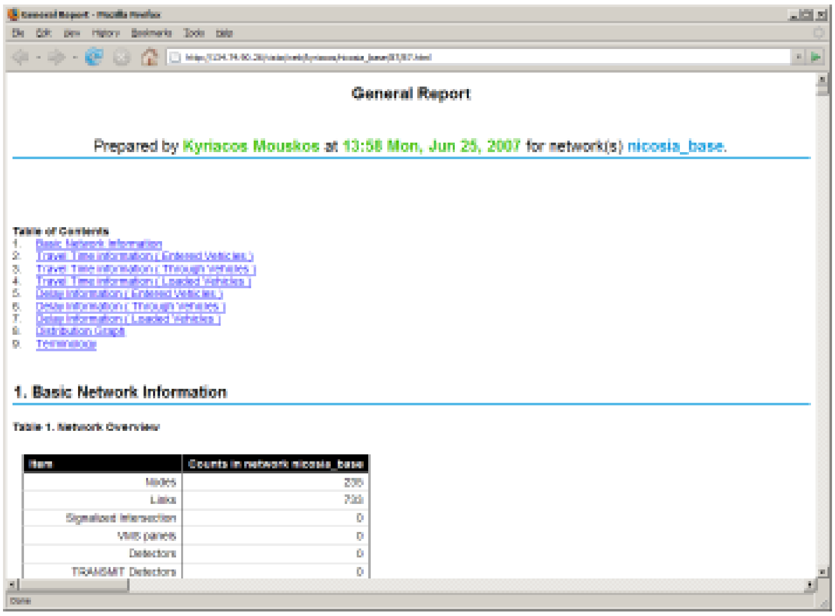
The EM Tool combines the Incident Management Module with the Dynamic Message Signs (DMS) module and includes the Emergency Services vehicle data. The DMS module produces the path travel times for the original and diversion routes and the corresponding number of vehicles that followed each route. The Incident Management Module outputs the incident report, which is an automated report that provides network-wide results related to the incident. A comparative analysis of the network under normal and incident conditions is reported. In addition, the distribution of vehicles that benefited or dis-benefited from the incident is also provided using the travel time and the corresponding delay, where a negative delay indicates a benefited trip travel time or delay.

The IAT and VISTA transport networks have the same GIS and network links. Where link numbering is different a correspondence table is generated such that the input from the IAT platform is accurately mapped to the VISTA environment. The input data required to execute the VISTA EM Tool are defined through the IAT user interface and communicated to the EM Tool through specific web-services.

IAT received the following output reports that are available for the EM module are:

1. General Report: The General Report provides the network-wide performance under each scenario tested. Each scenario is represented in a new network version. The Security Analyst has the capability to compare two or more scenarios per output report. The General Report gives general network statistics, such as number of nodes, links, controls and OD pairs. It also gives aggregate travel statistics including total system travel time and average, maximum and minimum OD travel times. It further provides the distributions of OD travel times and vehicles departure times. A sample of an automated General Report is portrayed in Figure 18.

   The General Report is a table that can be directly exported in Excel format.



General Report

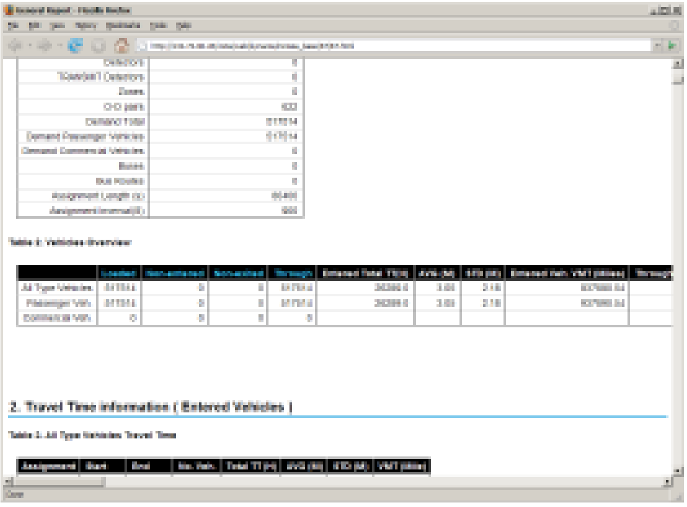
Prepared by Kyriacos Mouskos at 13:58 Mon, Jun 25, 2007 for network(s) nicosia_base.

Table of Contents
1. Basic Network Information
2. Travel Time information (Entered Vehicles)
3. Travel Time information (Through Vehicles)
4. Travel Time information (Loaded Vehicles)
5. Delay information (Entered Vehicles)
6. Delay information (Through Vehicles)
7. Delay information (Loaded Vehicles)
8. Distribution Graph
9. Terminology

1. Basic Network Information

Table 1. Network Overview

Item	Counts in network nicosia_base
Nodes	235
Links	733
Signalized Intersection	0
VMS panels	0
Detectors	0
TRANSMIT Detectors	0



Detectors	0
[illegible] Detectors	0
Zones	0
O-D pairs	[illegible]
Demand Total	[illegible]
Demand Passenger Vehicles	[illegible]
Demand Commercial Vehicles	0
Buses	0
Bus Routes	0
Assignment Length (s)	[illegible]
Assignment Interval(s)	[illegible]

Table 2: Vehicles Overview

	Loaded	Non-entered	Non-exited	Through	Entered Total TT(h)	AVG (h)	STD (h)	Entered Veh. VMT (Miles)	Throug
All Type Vehicles	[illegible]	0	0	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	
Passenger Veh.	[illegible]	0	0	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	
Commercial Veh.	0	0	0	0					

2. Travel Time Information (Entered Vehicles)

Table 3: All Type Vehicles Travel Time

Assignment	Start	End	No. Veh.	Total TT (h)	AVG (h)	STD (h)	VMT (Miles)

Figure 18: General Report Sample

2. Incident Report: This is an automated report that provides network-wide results related to the incident. A comparative analysis of the network under normal and incident conditions is reported. In addition, the distribution of vehicles that benefited or dis-benefited from the incident is also provided using the travel time and the corresponding delay, where a negative delay indicates a benefited trip travel time or delay.

   The Incident Report is a set of tables that can be directly exported in Excel format.

3. ES Vehicles Report: This is an automated report that provides path related data for each ES vehicle that responds to the incident. The ES vehicles report is provided via the OD travel time automated report that produces the corresponding OD travel time and the associated followed path.

   The ES Vehicles Report is a table that can be directly exported in Excel format.

1.3.4 Demonstration and Evaluation Results

The evaluation effort initiated with the definition of the evaluation framework. Its goal was to define the methodological framework that is applied during the evaluation as well as reach decision on specific aspects of evaluation. It defined and provided guidance on the following aspects of evaluation:

- **Evaluation Objectives**: It set out that what information partners wanted to obtain from the evaluation. Partners decided that evaluation would examine the functionality of the IAT, the intuitiveness of the underlying risk assessment framework as well as the overall marketability of the STAR-TRANS results. STAR-TRANS outputs which were not directly visible by the end user would be evaluated indirectly.
- **Evaluation metrics and instruments**: The project defined the specific indicators to be used for the evaluation of IAT. These indicators were formulated into questions and were compiled into a questionnaire which formed the STAR-TRANS evaluation instrument.
- **Trial participants**: The STAR-TRANS audience is comprised a small number of risk assessment professionals. In order to ensure a sufficiently high response rate, stakeholders were profiled and identified early.
- **Evaluation process**: An outline for the evaluation process was defined. Partners wanted to be able to integrate and compare results from different events. A scenario based approach was followed. Scenarios were defined for both Bologna and Athens which were presented to the end users during workshops. The familiarity participants have to these types of scenarios would be used to facilitate understanding the risk analysis frameworks and IAT. Following initial demonstrations, trial participants were given time

to interact with IAT and then asked to complete a questionnaire. To ensure high response rates, facilitators were on hand to assist with questionnaire completion.

- **Trial Preparation**: Matters of practical nature were listed in order to address them beforehand. Even though, IAT did not require installation, since, it is a web based service browser and internet bandwidth requirements were specified. Facilitator training was organized.

The overall evaluation execution included two major evaluation events one in Bologna and one in Athens which occurred on March and April of 2012 respectively. Prior to the evaluation events the consortium made contact with relevant STAR-TRANS stakeholders and end-users, briefed them on the project's scope and objectives and asked for their participation. Comprehensive scenarios stemming from the operational experiences during the Bologna Massacre and the 2004 Athens Olympic games were developed and tested. During the trial events the STAR-TRANS concept, goals and approach were presented to the participants along with a test scenario which was used to introduce them to the functionality, mind-set and workflow of the IAT. Subsequently, the end-users were handed out a questionnaire/evaluation form to fill out expressing their opinion and view on the project's results. Questionnaires were collected and compiled for data analysis.

Trials in both locations were executed with fully functional prototypes while the prototype in Athens had been upgraded since the event in Bologna in response to comments received. Furthermore, the experience from the Bologna trial was utilized to improve the trial flow ensuring that information delivery was optimized. Additionally, the focus of the events was different with the Bologna trial focusing more on the quality of results while the Athens trials paid attention more to the end user acceptance. Feedback to both rounds was rich and comprehensive. Due to the smaller audience in Bologna a more open and direct discussion took place. In Athens the presentation of the results from the Bologna trials were incorporated in the presentations. The larger and more international audience allowed for more responses to be collected. None of the participants had prior exposure to STAR-TRANS and IAT. Therefore, in both events responses collected expressed the opinions of first time users.

The events attended in total 36 district participants from 6 countries (i.e. Cyprus, France, Greece, Italy, Luxembourg and Serbia). They represented transport operators, public authorities, security experts and first responders. Overall the trial events were successful in collecting qualitative and quantitative end user feedback. They were opportunities for end users to interact with the STAR-TRANS consortium, get educated on the project's results and discuss with the consortium project results.

Trial participants thought that IAT is an interesting solution to a problem faced by many security related services and agencies. The capacity to mainstream the risk assessment process, explore the inherent risk of different scenarios on the entirety of the network of network, manage resources and estimate the optimal path of responders in order to minimise response time based on traffic simulation models is a welcome addition for the majority of the STAR-TRANS end-users. It is also a solid foundation upon which future solutions can build upon to extend this functionality. The end-users were quick to recognise the functionality that STAR-TRANS offered and reacted with a rather enthusiastic attitude towards suggesting additional features for future development.

1.4 Potential Impact and Main Dissemination Activities and Exploitation of Results

1.4.1 Project Dissemination

Dissemination covers actions supporting partners during the project and fostering their collaboration, on the one hand, and activities promoting the projects' results towards the outside world, on the other hand. STAR-TRANS's strategy has been to treat dissemination equally as a communication and working tool. Dissemination activities are intended to promote the project and its results beyond the consortium but also to support trials and feedback collection by inviting stakeholders and establishing relationships with them. Additionally, dissemination serves as diffusion processes or mechanisms promoting the project's exploitable results thus identifying and approaching potential clients to assess market attractiveness of STAR-TRANS project results.

Strategy

The approach to dissemination is threefold:

- *Continuous* as it runs throughout the project's life;
- *Ubiquitous* as it relates to all working packages' activities and is consubstantial to all activities;
- *Flexible* as it is adapted according to the project's findings and the partners' needs.

Dissemination Methodology

In order for the dissemination to be effective and to provide tangible results, a well-structured methodology was adopted in terms of:

- Defining the main objectives of the dissemination strategy, e.g. promoting the STAR-TRANS idea, objectives and results to all potential stakeholders.
- Identifying the target groups for dissemination, i.e. to disseminate the work carried out, knowledge produced and results achieved to the wider possible audience.
- Establishing the appropriate source for the dissemination activities (in terms of roles and responsibilities).
- Raising public awareness on the project achievements through the most suitable means for communicating with the respective target groups.
- Defining what messages are disseminated to the public.

Dissemination Objectives

The objectives of dissemination activities are to:

- Build the identity of the project and promote the STAR-TRANS' name;
- Give a structure to the main activities of the consortium and thereby spread knowledge gained during the development of the project among partners;
- Create awareness of the project's results for the different interest groups that may extend beyond the project's immediate targeted audiences;
- Promote the STAR-TRANS ideas, objectives, exploitable and scientific results of the project;
- Attract users to the new service, trials and events;
- Engage users and targeted stakeholders in the project's acceptance.

Consequently to the definition of dissemination, activities are directed both:

- towards partners, to support them in building the project's identity and working processes;
- towards non-partners, to serve as a tool in order to approach and convince them. Dissemination activities are of a promotional nature so as to address targeted non-partners for business opportunities and future partnerships.

Target Audience

Dissemination activities target all organisations that are:

- Involved in responding to risk incidents in surface transport systems;

- Ensuring business continuity of transportation networks;
- Active in developing solutions capable of analyzing risks affecting road transport systems;

Dissemination activities target both public and private organisations such as the following:

- Public Authorities (policy makers, public safety agencies, emergency responders, security agencies, critical infrastructure operators and protection agencies, national authorities for transport / security / active in responding to risk incidents and ensuring business continuity of transportation systems): End user organizations led dissemination efforts in this target group. They understand the needs and constraints of these stakeholders and can better present the benefits of the STAR-TRANS outcomes. Moreover, they possess the experience and credibility to discuss STAR-TRANS in terms of strategic and operational of risk assessment and emergency response contexts.
- Universities and research institutes: Research organizations in the consortium focused on disseminate project results on a research level. They have extensive knowledge on the state-of-the-art relevant to STAR-TRANS and broad experience in participating to major events and conferences with remarkable scientific contribution. These partners guide project dissemination activities in this area, in order to successively target the research groups with potential interest on the project scientific achievements.
- Private industrial partners such as insurance companies, associations representing transport and/ or security related stakeholders: Industrial partners identified and established contact with potential end user of the project results. Communication included dissemination of project developments and results as well as solicitation of feedback and broader discussions.

All activities promoting the exploitable results of the project and aiming directly or indirectly at fostering an exploitation strategy and business plan are supported. Therefore, special attention is put on dissemination towards those organisations interested in investing into the project's end-results and developing its solutixz

The targeted geographical coverage of STAR-TRAN's dissemination plan includes all European Member States. The coverage is not restricted to the European Union only. Select events are used to bring the STAR-TRANS message to the international community.

Even though, STAR-TRANS evaluated the proposed Risk Assessment Framework in two demonstrators using the Athens and the Bologna transportation networks, special attention was paid not to limit the geographical coverage of dissemination activities to Bologna and Athens. After contacting, the primarily interested parties be those directly involved in the Bologna, for the Athens demonstrator international participants were invited. Attendees were from 6 countries. As STAR-TRANS results are neither geographically confined nor limited to the specificities of one city's transportation system an international coverage is appropriate.

Dissemination Channels

The following channels, supporting partners and/or communication towards non-partners, are to be used:

- **Logo**, representative of the project's concept and vision;

- **Templates** for Word and Power Point building on the project's logo;

- **Website**, functional and user friendly serving as a major dissemination tool to present the project and news; Project Website USRL: http://www.startrans-project.eu ;
- **Project fact sheet,** used by partners to present the projects facts in writing;
- **Project Presentation,** used by partners when presenting the project or disseminating the project
- **Leaflets and Posters**, two sets of leaflets and posters were designed and produced - the first set early in the project disseminates project objectives, concepts and vision of STAR-TRANS; the second during the third year of the project presents disseminate public results, outcomes and findings from STAR-TRANS research / this material is used in all public events (conferences, workshops, exhibitions, etc.), where STAR-TRANS Partners participate;
- **Forums / workshops** serve as major dissemination events, where all developments and concepts of STAR-TRANS are analysed, discussed and disseminated to relevant user groups, the general public as well as internationally (outside Europe. Two workshops were organised: one to discuss and debate project's concept and initial findings with stakeholders in order to promote the STAR –TRANS system and validate the approach with stakeholders (e.g. public safety agencies, security agencies, critical infrastructure operators), that can act as leverage for the market creation. The second workshop presented the STAR-TRANS system to stakeholders, and collected feedback to assist the planning of the future activities;
- **Articles** in specialized press using the partners networks and contacts;
- **Participation to conferences** focused on security and risk assessment (emphasis is placed on appropriate selection of the information provided, on a clear and to the-point presentation and on the protection of specific know-how of the project partners.
- **Liasons with other projects** active in the same areas as STAR-TRANS were established**.**
- **Wikis** disseminating project results to the broader technical community such as the dissemination STML

Main Messages

STAR-TRANS benefits from the repetition of one single message which includes the following elements:

- STAR-TRANS offers benefits related to public safety;
- STAR-TRANS aims at assessing risks affecting European interconnected transportation networks, known as 'the network of networks';
- STAR-TRANS builds tools capable of understanding how risk incidents occurring in one single transportation system are capable of affecting the transportation network as a whole;
- STAR-TRANS' applications are not limited to the specificities of one single city;
- STAR-TRANS creates exploitable results in the form of a software;
- The European Commission supports the project through FP7 funding.

The STAR-TRANS motto is "Assessing risks affecting EU interconnected transportation networks".
Accompanying the project promotional message included information relating to project results. More specifically:

- The knowledge of the Transportation Security Risk Assessment Domain and the Risk Analysis Framework introduced to structure and homogenize the approach to risk assessment.

- The definition of user needs requirements, constraints and demands specifications.
- Technical know-how relating to the design, development, testing and deployment of the Impact Assessment Tool including IAML and STML.
- Results from the project evaluation such as user comments and analysis.

Special Clause 24 Limited Dissemination of Foreground Outside the Consortium for Security Reasons

The project is subject to Special Clause 24: "Any foreground, generated in the course of the project shall not be disseminated to any legal entity outside the existing consortium, unless agreed otherwise by the beneficiaries and the Commission. This rule also applies to affiliates or parent companies." The project did not produce any security rated foreground. All foreground was based on publicly available sources (i.e. published research or public GIS information) or sources which did not carry a security rating.

1.4.2 Project Outcomes Exploitation

Building on three years of research and development, STAR-TRANS project responds to a pressing need – and opportunity – to strengthen the overall security management of interconnected and interdependent transport networks.

Exploitable Results

STAR-TRANS' has introduced a solution that benefits the whole transport security system; national authorities, private companies and non-governmental organisations operating within transport and/or security domains. The solution is based primarily on the Impact Assessment Tool (IAT) which facilitates the application of the Risk Analysis Framework and utilizes STML Engine Core and VISTA systems.

IAT allows its users to risk assess any land based transportation network of networks. Tool operations have been conceptually split in four different and discrete tools which are described in more detail in the following sections:

5. The **Network Modelling Tool (NM)** that handles the representation of the transportation network, describing its assets and their interdependencies as well as modelling the network of networks and their interdependencies.
6. The **Risk Modelling Tool (RM)** that allows the description of threat scenarios and represents them as networks of primary and propagated incidents and consequences on assets. Through the use of VISTA, it allows the visualization of traffic conditions resulting from the threat scenario.
7. The **Risk Analysis Tool (RA)** which reports the results of risk analysis and facilitates decision making to ensure that realistic targets and commitments are established.
8. The **IAT Administration Tool (IA)** that manages the input of historical data, impact propagation matrix, threat – consequences matrix and other important data for the risk evaluation process, as well as user profiles, roles and authorization.

The software tool provides the technology to link together relevant assets of interconnected and interdependent transport networks, such that risk managers, policy makers and others can, subsequently, be provided with the impact that a risk incident on an asset of a specific transportation network may have on the assets of other interconnected and interdependent transport networks. Special attention is given to the intuitiveness of the user interface, the responsiveness of the system and its security.

Products and service variations

This section outlines 3 service variations based on the STAR-TRANS exploitable results which can be applied when commercialising project outcomes.

- ***Package 1 - Access to a web-based service:*** Under this package, a customer would buy an access to the web-based service of the IAT.
- ***Package 2 - Access to a web-based service and building the Network of Networks (NoN):*** In addition to the first package, the client network of network is developed and imported into IAT for them. Where the client would have to gain the experience amassed in the project, the STAR-TRANS entity has the assistive tools, exeprtise and experience to accomplish this task at faster and at a lower cost.
- ***Package 3 - Access to a web-based service + consulting and value added services:*** In addition to the access to the service and building of NoN, STAR-TRANS will offer other services such as technical support, building of customers' models, entering the clients' networks, training, maintenance and expert opinion linked to the use of the functionality. This package could offer also integration of all required data related to the characteristics of the specific network and to support them in using the tool.

Project evaluation demonstrate that the most preferable service that the end-users is the online access to the IAT services. However, strong demand was expressed for staff training, technical support, incorporation of the functionality into their network/back-office systems and software maintenance in order of most to least importance. Local installation and provision of content analysis were the least favoured options. These results indicate potential customers understand very well risk analysis, however, they lack the will to undertake the IT component of the service. Therefore, the 3 packages offered become more attractive according to the level of experience, the user has with the system.

Marketing strategy

To implement successful business case, it is important that STAR-TRANS offers the right product/services in the right place at the right time. There are a range of marketing solutions that can help to generate a reasonable income. Keys to success are:

1. ***STAR-TRANS's services must be able to acquire and retain customers by following a defined marketing strategy;***
2. ***The IAT must be easy to use and fully interactive. User satisfaction and measurable results are ultimate priorities;***
3. ***The sales process must be easy to administer and with a flexible pricing policy to accommodate the users' needs.***

With regard to point one, STAR-TRANS set up a User Forum early in the project to obtain input and feedback from stakeholders. Furthermore, the acquired know-how will be integrated into overall marketing strategy and thus evaluation results and testimonials would be used as well. In parallel, **conferences and workshops** were used for presenting the IAT in order to attract attention. Finally, visibility of the IAT was ensured mainly via **internet marketing** (target mailing lists, "Search Engine Optimisation", "Search Engine Marketing", use of social media, etc.).

The STAR-TRANS consortium aims to exploit project results through flexible pricing. Four pricing options were examined during the project:

1. One-off payment: this is a onetime payment for unlimited access to IAT. This is emerged as the proffered payment method for end users as it is the most convenient.
2. Annual license: a fee payable every year was proven to be the least popular option among the evaluation responders. When usage volume is minimal, this pricing model is the most appropriate.
3. Pay per use: payment extracted for each assessment run using IAT. The model is most profitable when the client wants to run multiple alternative scenarios which require assessment.

4. Per licence/user fee: payment for each person using IAT irrespective of how many assessments they executed. This pricing is most profitable when the risk assessment role is fragmented to multiple employees within the organization.

Potential Customers

Transportation networks, perceived as critical infrastructures, form a vital part of the European economy and society. While governments remain ultimately responsible for maintaining the stability and prosperity of the economy and the society, a key responsibility for their implementation typically rests with private sector stakeholders who operate most of the transport networks and have the expertise to protect them. This public – private relationship is further complemented by interactions of voluntary and non profit sector.

1. Public authorities: policy makers, law enforcement agencies (police), fire brigades, ambulance services, special health advisory teams, coastguard, local authorities, military assistance, civil protection and other public entities active in the management and understanding of European transportation networks and incidents affecting them
2. Enterprises: private companies supporting public organizating securing and ensuring the resiliance of transportation networks.
3. Non-profit organisations: NGOs involved in the sectior.

The potential customer will use IAT to assist them in Incident Responce Planning, Impact Assessment, Critical Infrastructure Identification, personnerl training and providing guidance during an emergency.

Business structure

Partners have agreed to commercialise project outcomes by forming a separate business entity. They will contribute to this entity according to their role and involvement in the STAR-TRANS project. Issues related to responsibilities of parties; liability towards each other; governance structure; access rights; foreground and finances will follow the similar principles as outlined in the Consortium Agreement.

1.4.3 Societal and Economic Impact

The proposed STAR-TRANS actions in the area of transportation security provide the technological basis and relevant knowledge needed in security capabilities. Project outcomes were developed through close collaboration with industrial and public sector end users, and promise a significant improvement with respect to performance, reliability, speed and cost. The successful implementation of STAR-TRANS reinforces the European industry's potential to create important market opportunities and establish worldwide leadership, and it ensures sufficient awareness and understanding of all relevant issues for the take-up of their outcome.

STAR-TRANS addresses the need to identify the risks and vulnerabilities of critical infrastructures located in the EU Member States and transnational ones, damage to which could have serious and wide-ranging consequences, as noted in SEC(2005) 436 "Annex to General Programme Security and Safeguarding Liberties". And even though, it does not directly propose measures to be taken to reduce this risk, it provides the methodology and ICT tools to do so. Through practices which integrate the use of STAR-TRANS' outcomes, policy makers and practitioners have the ability to identify best practises and unintended consequences of incident response procedures at a wider area of scope, the network of networks. The capacity to undertake these tasks and to implement the preventative measures concerned, however, varies markedly across the EU, and the introduction of a harmonized holistic approach is a key initiative within STAR-TRANS.

The outcome of the STAR-TRANS project is expected to contribute towards the development of a common approach for risk analysis and perception initially in transportation critical infrastructures, that can be further upgraded into a common strategic level tool for the design and analysis of surface transportation systems.

Specifically, within STAR-TRNAS a wide range of possible security related risk incidents likely to happen on transportation networks at European level were analysed and treated on a strategic level, allowing for consideration of the optimal planning decisions that will allow for the minimization of the perceived risk, and better preparedness of emergency responders and transport operators alike in the event of such incident.

STAR-TRANS could be pivotal towards in the acceptance of a common and holistic risk management methodology across EU countries, and develop adequate standards and procedures for the harmonised implementation of solutions and services consistent with the defined (across countries) framework.

Furthermore, introduced a common risk analysis approach where risk is propagated between interconnected and heterogeneous transportation networks. Therefore, the operator / security manager of a transport network would not perceive risk only the ones pertaining to its own network, but would capture 2nd order effects from incidents initiating into different transportation networks.

STAR-TRANS is consistent with the Commission's initiative on security and in particular with the "Green Paper on a European Programme for Critical Infrastructure Protection" [COM(2005) 576 final, 17.11.2005]. In this context the protection of key sites and monuments is also of concern due to their high symbolic and societal value. The Green paper endorses harmonization and integration of methods and standards for vulnerability and risk assessment through benchmarking, active networking and stakeholder involvement. In accordance to the aforementioned activities, STAR-TRANS focused on:

(a) development of an improved framework for risk analysis and vulnerability assessment methods related to the transport sector;

(b) identification, study and harmonization of best practices and supporting methods and tools for emergency preparedness and response to accidents;

(c) development of a state-of-the-art service-oriented software architecture for integrated transportation vulnerability assessment and risk management.

Since a failure of one Member State's transport infrastructure can affect the infrastructure of another Member State, it is clear that such critical infrastructures with a trans-national dimension should be identified and designated as European Critical Infrastructures (ECI). The trans-nation dimension of transportation within the EU demands a common procedure concerning European Critical Infrastructures (ECI) identification and assessment. Therefore, transportation security risk assessment addressing transnational transportation vulnerabilities complements national programs and adds value to the continued viability and wealth creation capabilities of the European internal market. STAR-TRANS has an instrumental role to play in the establishment of a common list of transnational critical infrastructure through its framework. The framework provides the necessary basis for a coherent and uniform implementation of measures to enhance the protection of Transport Networks, as well as defining clearly the respective responsibilities of Transport stakeholders.

The proposed methodology viewed risk analysis from the perspective of both the network operator and emergency responders and emphasizes jointly the reduction of the impacts on business continuity, and human losses, economic and societal impacts. To this extend, STAR-TRANS could provide strategic level analysis for the implementation of security solutions and services by embedding them in the conception of existing / upgrade/ new infrastructure, while taking efficiency, business and societal constraints into account.

Additionally, the risk framework has been linked to the VISTA Dynamic Traffic Assignment model providing realistic simulation results on several aspects of the response and recovery process including the ability to capture the combined time varying routing choices accounting for every conceivable control, supply and demand needs, such as evacuation, route diversions, and optimal paths of emergency vehicles.

Furthermore, STAR-TRANS project is linked to Directive 2008/114/EC on Critical Infrastructure Protection. This directive lays down that each Member State must ensure that an Operator Security Plan (OSP) or an equivalent measure is in place for each designated ECI. The Operational Security Plan, imposed by Directive 2008/114/EC, provides concrete operational procedures which are applicable to any transport network given. However, they must be used in parallel with the necessary data describing the significant assets. Such operational procedure, which aim is to improve the organisational results regarding the protection and continuity of transport networks, should consist of the following steps:

1. Identification of important assets
2. A risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact is conducted.
3. Identification, selection and prioritisation of counter-measures and procedures
4. Appointment of responsible person
5. Appointment of ECIP contact point

The STAR-TRANS IAT can be directly used to target the implementation of points (1-3) above in an user friendly and time saving manner, allowing for the analysis and thorough examination of a very large number of scenarios in significantly less time. Therefore it could prove a valuable tool for the critical infrastructure operators, national authorities for the protection of critical infrastructures and emergency responders to reduce possible security incidents to critical transportation networks.

STAR-TRANS has specific examples on potential impact its outcomes can have on an organization. SRM is a public transport authority and owner (together with local governmental bodies) of transport networks data. Furthermore, the local competent bodies delegated to SRM the functions to award the public transport bus service The scenario delivered for Bologna allowed to SRM to start contacts with the bodies responsible for safety and security issues in the city (Civil Protection and Police), in addition to public transport operators (bus and railways).

1.4.4 Lessons Learnt and Future Work

1.4.4.1 Lessons Learnt

STAR-TRANS highlighted once more the need for the European Union to develop a common policy across all countries to develop a common data model for transport data. The unavailability of such a data model leads to the following deficiencies:

1) Different geospatial coordinate systems needing a special transformation code to move from one GIS system to the next; especially the Athens data required several weeks until such data transformation code was developed;

2) Historical data gathering is slow and beurocratic process as data are owned by several agencies belonging to different ministries;

3) Traffic data updated infrequently and uniformly around the transport network leading to deficiencies in the calibration of static and dynamic traffic assignment models.

An EU directive - supported by adequate funding – is necessary to develop a transport data model, which will include the data specifications, GIS EU format, data collection, updating and storage procedures, and an efficient protocol for all public agencies to store their data into a publicly available data warehouse. Such a data model will provide consistency among studies conducted on the same network, streamlining the calibration of various models using the same data, allowing proper comparisons among models and removing the need for requesting data from many different transport agencies.

1.4.4.2 Future Work

Critical transportation infrastructures may be owned, operated and protected by a variety of public, private and hybrid entities. This complexity inevitably raises security challenges, in terms of allocating responsibility for prevention and response to threats or incidents and coordinating the use of resources. Therefore, the introduction of STAR-TRANS as a reference solution could provide the common ground for developing common and harmonized Operator Security Plans (as indicated in Directive 114/2008) based on the concept of interconnected critical infrastructures where risk is propagated between networks.

The STAR-TRANS approach could be developed, into a simulation based platform, that will provide critical infrastructure owners/operators and emergency responders a platform for conducting training and realistic exercises on a regular basis, examine new concepts and evolving security threats. The definition of Key Performance Indicators, will aid the participating organizations in defining /upgrading optimal response procedures especially, if the STAR-TRANS modeling framework is enhanced with a multiobjective optimization process.

Also, a major improvement of STAR-TRANS will be to expand its approach into interconnected critical infrastructures of different sectors (e.g. energy, chemical industry) employing the "network of networks" concept where risk and security incidents are propagated into heterogeneous and interconnected CI.

The IAT-VISTA collaboration can be expanded through the development of a continuously updated IAT-VISTA operational model such that it can be used to support emergency management at various cities, metro areas and networks around the world. This could take the forms of:

- a continuously calibrated VISTA DTA model. We note here that based on the current models that exist it is not feasible to execute a DTA model in real time as it requires a few hours to reach DUE convergence. The base model developed will be updated periodically based on the continuous online data.
- a real-time traffic forecasting system using only the VISTA traffic simulator. This is feasible as the trafic simulator is capable of running in a few minutes – as mentioned we cannot execute a DTA model to convergence in real time. The simulator will be using the latest set of DUE paths under the assumption that they will not change in real time.
- a real-time emergency vehicle routing model. Given the real-time traffic forecasting model, the corrsponding routing algorithms for each emergency vehicle could then be determined in real time.

1.5 Public Website and Contact Details

Coordinator	INTRASOFT International S.A.
Main Representative	Dr. Antonis Ramfos
Address	Rue Nicolas Bove 2b
Telephone Number	+ 30 310 6876482
Fax	+ 30 210 6876478
e-mail	Nikolas.athanasiadis@intrasoft-intl.com
Project WEB site address	www.startrans-project.eu

2 USE AND DISSEMINATION OF FOREGROUND

This section summarizes the plan for use and dissemination of foreground (including socio-economic impact and target groups for the results of the research). The dissemination and use plan describes and associates the STAR-TRANS Project outcomes (Knowledge of Transportation Security Domain, Risk Analysis Framework, IAML/STML and associated Engine Core, Impact