D'APPOLONIA

D'Appolonia S.p.A.
AN ISO 9001 AND ISO 14001 CERTIFIED COMPANY
www.dappolonia.it

A methodological approach for the identification and protection of critical transport infrastructures

24th May 2012

Table of Contents

- Definitions
- Identification of Critical Assets
- Protection of Critical Assets
- Instruments for the Demonstration of Security
- Conclusions

Definitions (1)

Transport EU-Critical Infrastructures:

Those physical resources and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States

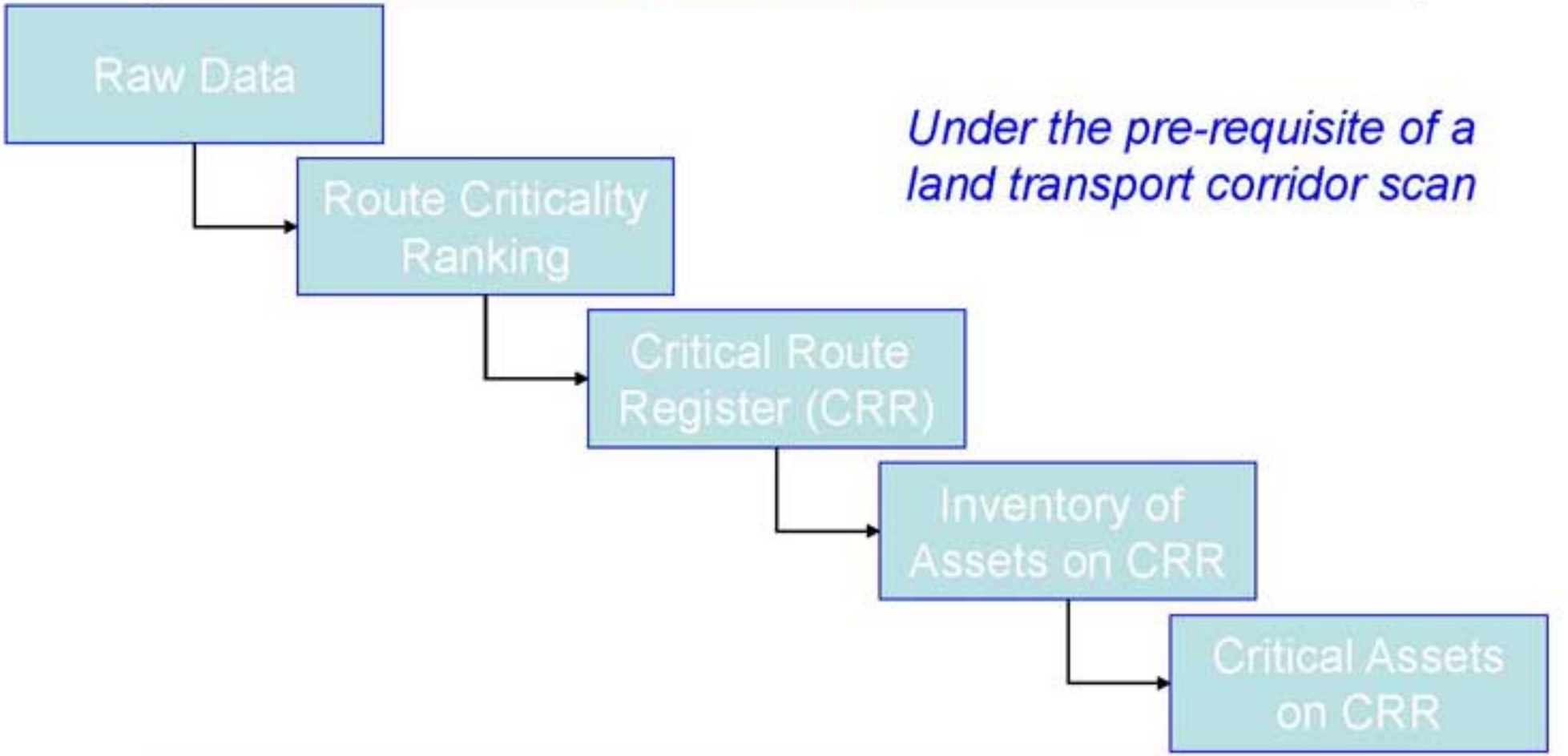
Definitions (2)

What is a serious impact?

From the literature of the most recent terrorist attacks to transport infrastructure and similar accidents to major transport assets, it is sensible to consider the following thresholds:

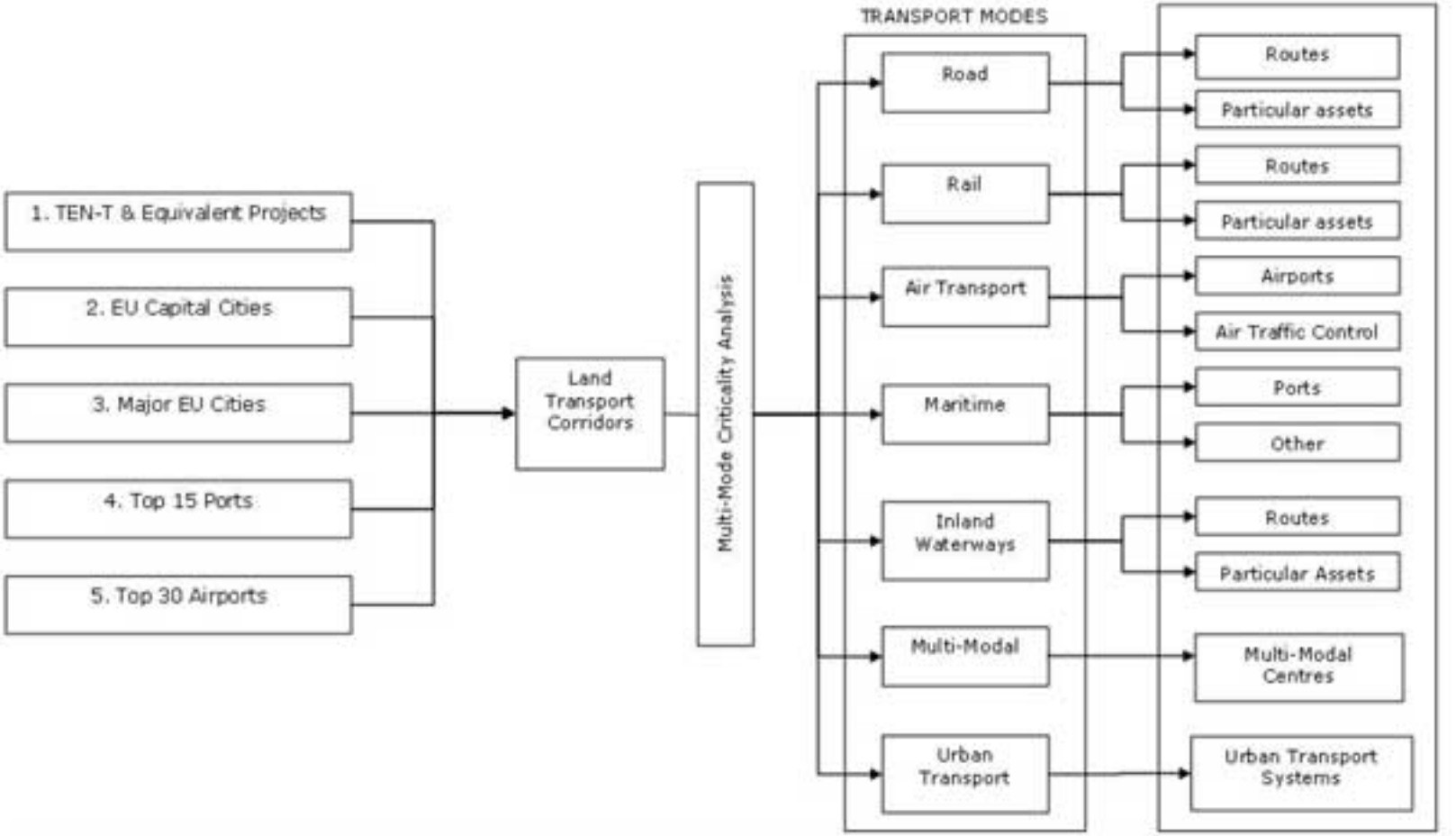
- Direct Impact Threshold: 0,25% of GDP
- Indirect Impact Threshold: 5% of GDP

Identification:
5 Basic Methodological Steps

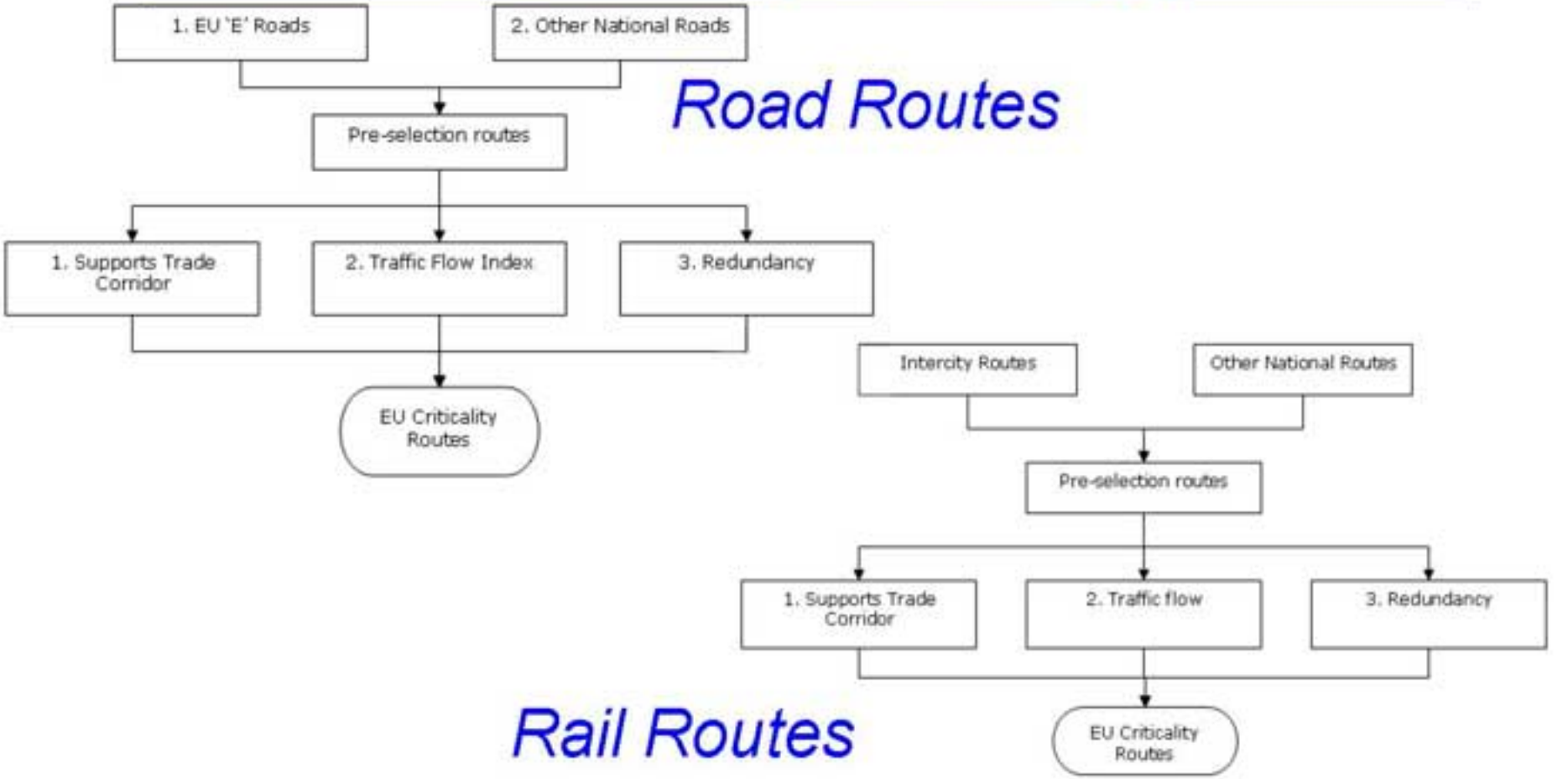


Under the pre-requisite of a land transport corridor scan

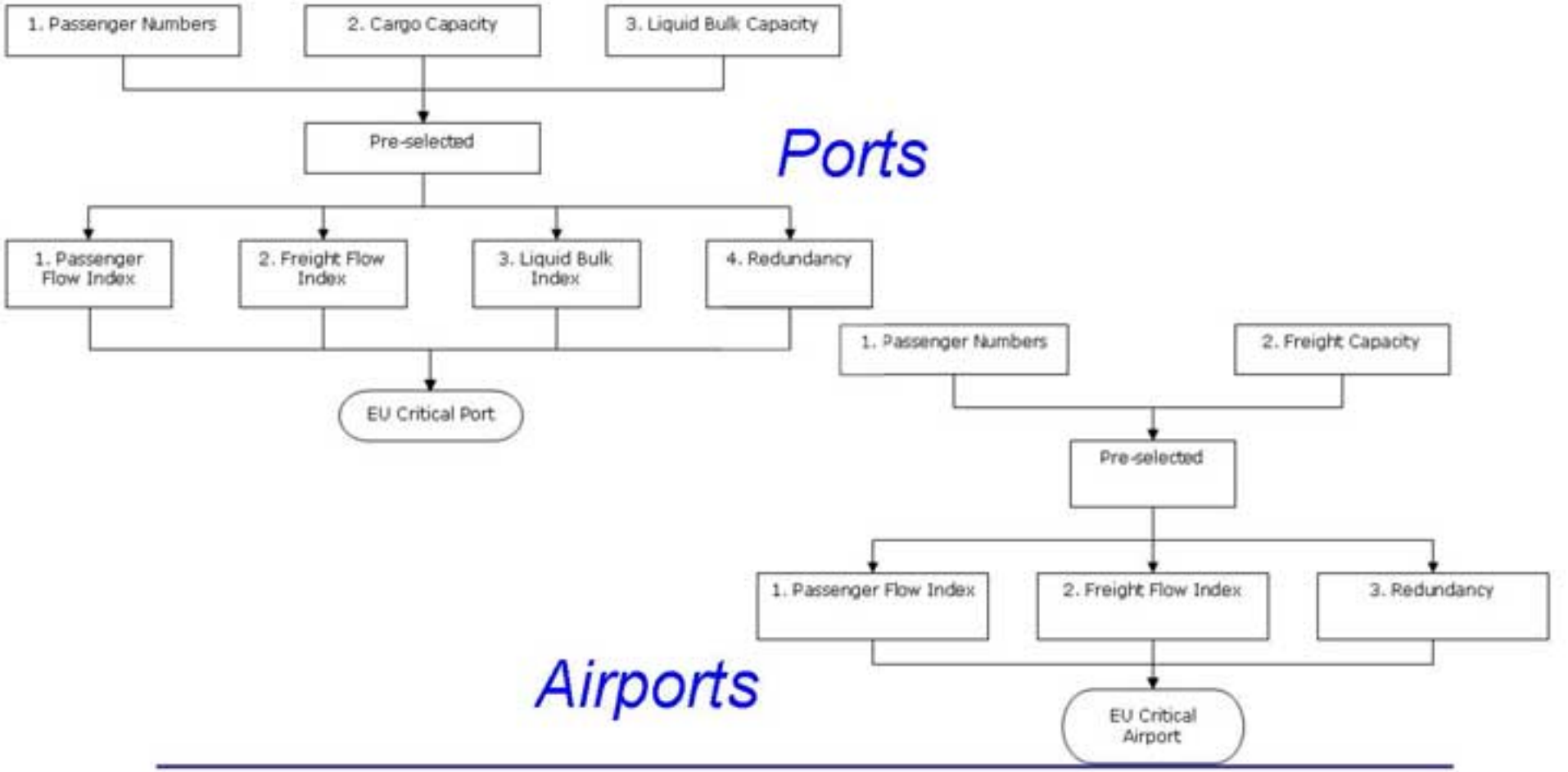
Identification:
Derivation on the Transport Modes (1)



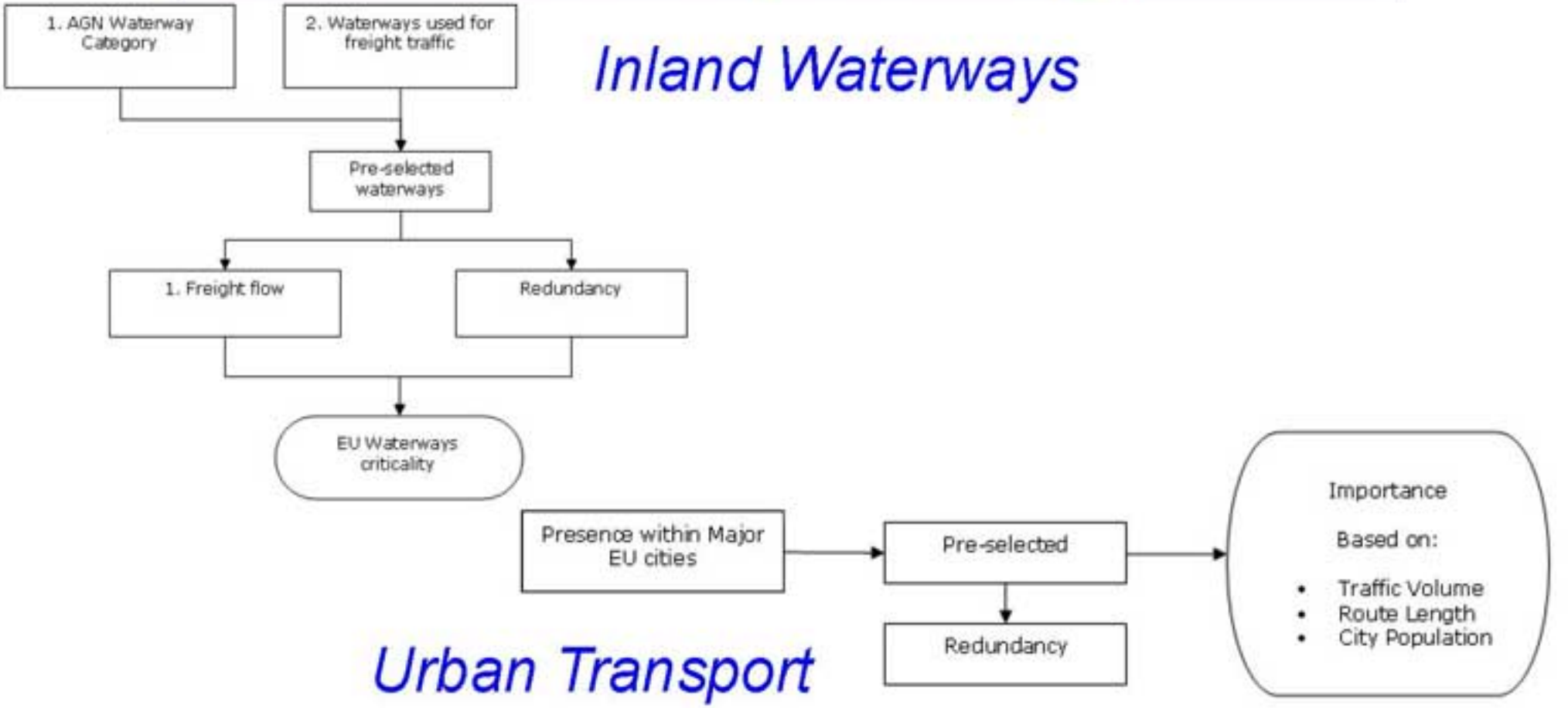
Identification:
Derivation on the Transport Modes (2)



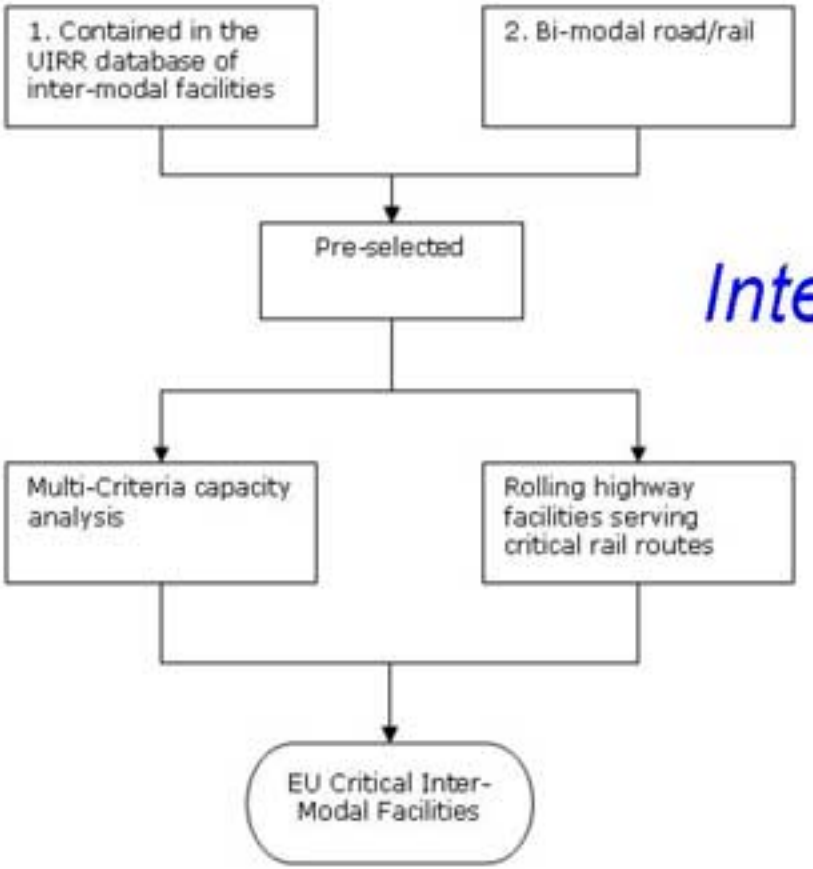
Identification:
Derivation on the Transport Modes (3)



Identification:
Derivation on the Transport Modes (4)



Identification:
Derivation on the Transport Modes (5)

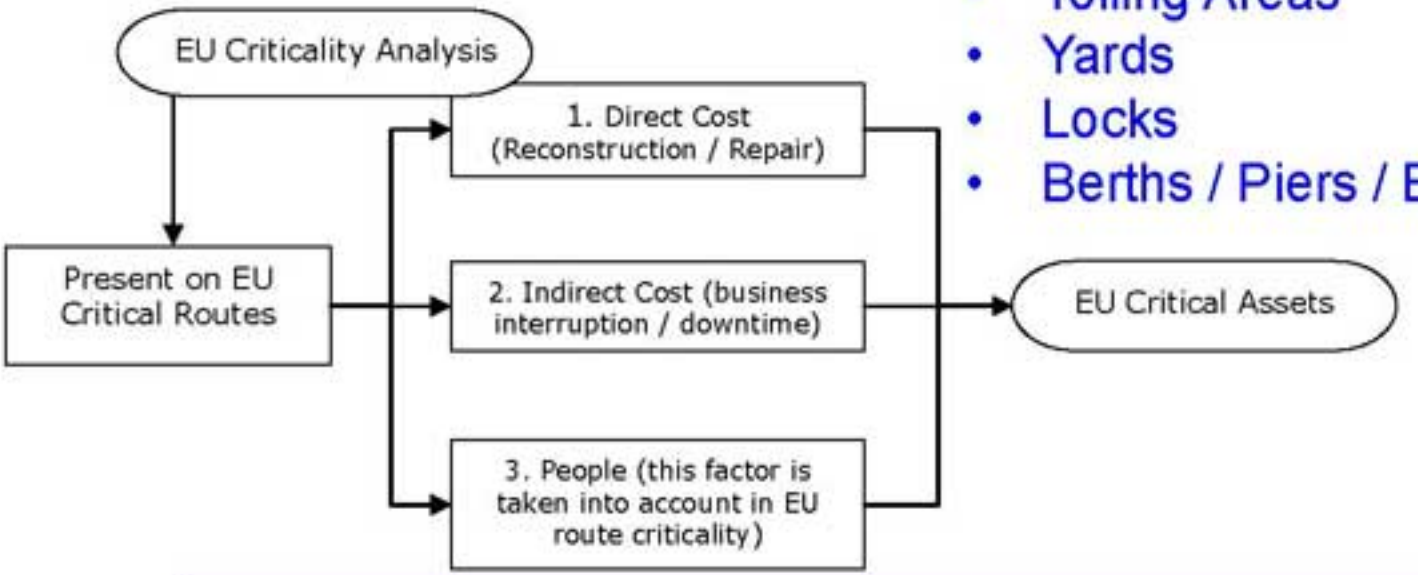


Intermodal Facilities

Identification:
Particular Asset Criticality

Assets include:

- Bridges / Viaducts
- Tunnels
- Traffic/Signalling Control Centres
- Stations
- Tolling Areas
- Yards
- Locks
- Berths / Piers / Embankments



Identification:
Ranking of the Assets

Proposed criteria:

- Presence on EU Critical Routes
- Asset specific features
- Size of structure, e.g. span
- Type of structure, e.g. suspended bridge
- Downtime / Business interruption
- Replacement / Repair cost
- Environmental impact
- Loss of life

Ranking of assets is possible on semi-quantitative basis.

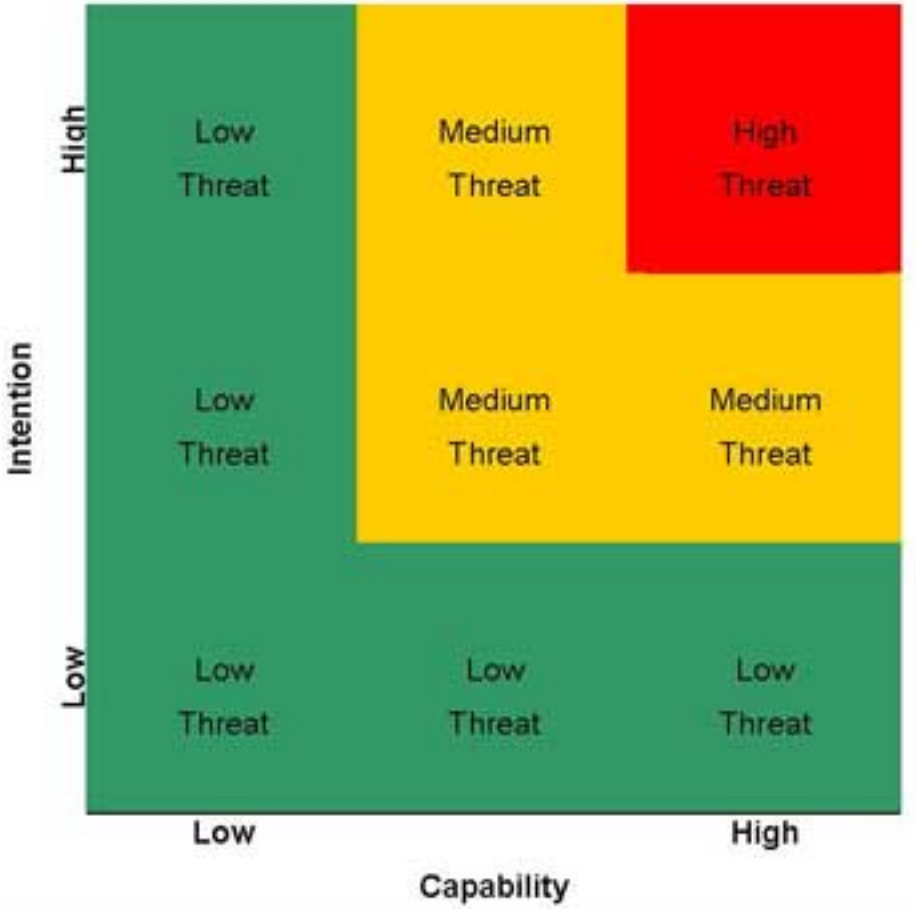
Protection:
Definining Security Risk

- **Risk** = Probability X Consequence

- **Probability** =
  (Threat X Target Attractiveness X Target Vulnerability)

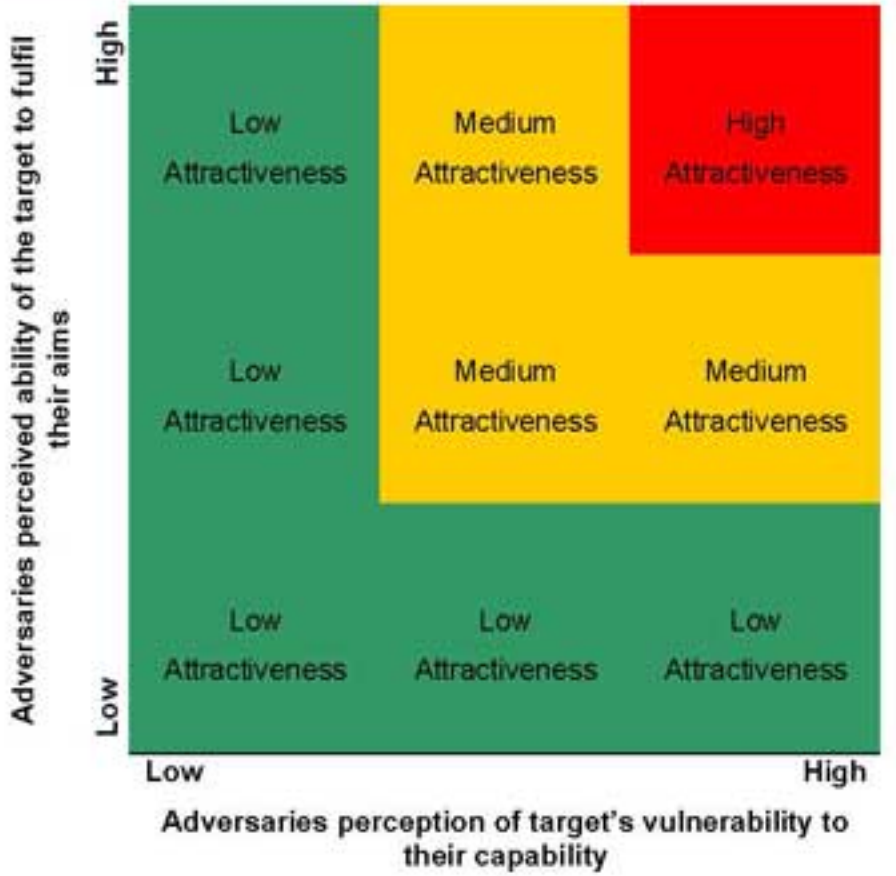
- **Threat**: underlying level of threat that is posed to the Member State where the asset is located
- **Attractiveness**: likelihood that the facility or asset is selected as target
- **Vulnerability**: target's inability to deter and withstand a successful attack
- **Consequences**: measure of the losses

Protection:
Definining Security Risk - Threat



The **Threat** describes the level of threat that a particular country considers itself to face

Protection:
Defininig Security Risk - Attractiveness



The **Attractiveness** measures the level of interest that a particular asset would have in the eyes of the adversary and consequently the likelihood or probability of it becoming a target

Protection:
Definining Security Risk - Vulnerability

- **Vulnerability**: target's inability to deter and withstand a successful attack. It is composed of:
  - Geographical Accessibility.
  - Threat Prevention (deterrents).
  - Consequence Reduction.
  - Target Hardness (resilience).

- The vulnerability score is estimated through a **Security Vulnerability Assessment** (SVA). This is a process that identifies the status of the vulnerability barriers via competent surveyor and is **related to attack scenarios**.

Protection:
Definining Security Risk - Consequences

	People	Financial	Environmental	Reputation
5	Extensive and serious injuries sustained (>100 fatalities)	>€1 billion	>1 million tonnes	Catastrophic
4	Extensive and serious injuries sustained (>10 fatalities)	€100 million – €1 billion	100,000 – 1 million tonnes	Major
3	Extensive and serious injuries sustained (<10 fatalities)	€10 million – €100 million	10,000 – 100,000 tonnes	Significant
2	Extensive and serious injuries sustained (single fatality)	€1 million – €10 million	1,000 – 10,000 tonnes	Notable
1	Minor injuries sustained (no fatality)	€100,000 – €1 million	100 – 1,000 tonnes	Minor

The **Consequence** evaluates the impact of a successful attack. Figures are indicative. Categories are to be combined weighted

Protection:
Risk Mitigation (1)

- **Risk mitigation** is the process of reducing the risk through application of **measures**, **countermeasures** and best **practices** in order to **reduce** the **likelihood** and/or the **consequences** of a successful attack
- Once mitigation measures are applied, the risk assessment should be recalculated to determine the **Residual Risk Profile**.
- The **Residual Risk Profile should record** a **level of risk** that is **acceptable** if the mitigation measures have had their desired intent

Protection: Risk Mitigation (2)

- Reducing likelihood (actual threat) includes the barrier processes which are responsible for the prevention of attack:
  - **surveillance cameras,**
  - **intelligence,**
  - **fencing,**
  - **security patrols** etc.
- Consequence mitigation are those barriers to **reduce the consequential impact** of a security attack which has occurred:
  - **fire and gas detection,**
  - **fire suppressions,**
  - **emergency response,**
  - **refuges and evacuation plans**
  - **business continuity plans**

Protection:
Risk Mitigation – Security Management System

- The management of the barriers is a fundamental process which must be controlled in a auditable manner. The **Security Management System** is a means of ensuring that:
- the barriers are sufficient in number
- the barriers are effective
- the barriers are readily available
- sufficient qualified personnel are available to ensure that the barrier integrity is maintained

- The Security Management System could be contained within a **Security Case** and visually represented and managed through the use of a **Bow Tie** process.

Protection:
Risk Mitigation – Security Case (1)

- Security Case could be developed and maintained to reflect current practice at the location or site and is endorsed by the asset owner/manager. It is composed of

  - Part 1 – **Management Summary and Introduction:** summary of the Security Case objectives, the main findings and security risks
  - Part 2 – **Security Management System for Location/Site:** A description of those corporate elements of the Security Management System that is directly applicable to the site
  - Part 3 – **Countermeasures/Recovery Procedures Catalogue:** A description of those security countermeasure and recovery procedures at the site. This is recorded to show that the controls are in place, suitable and sufficient for the security risks addressed.

Protection:
Risk Mitigation – Security Case (2)

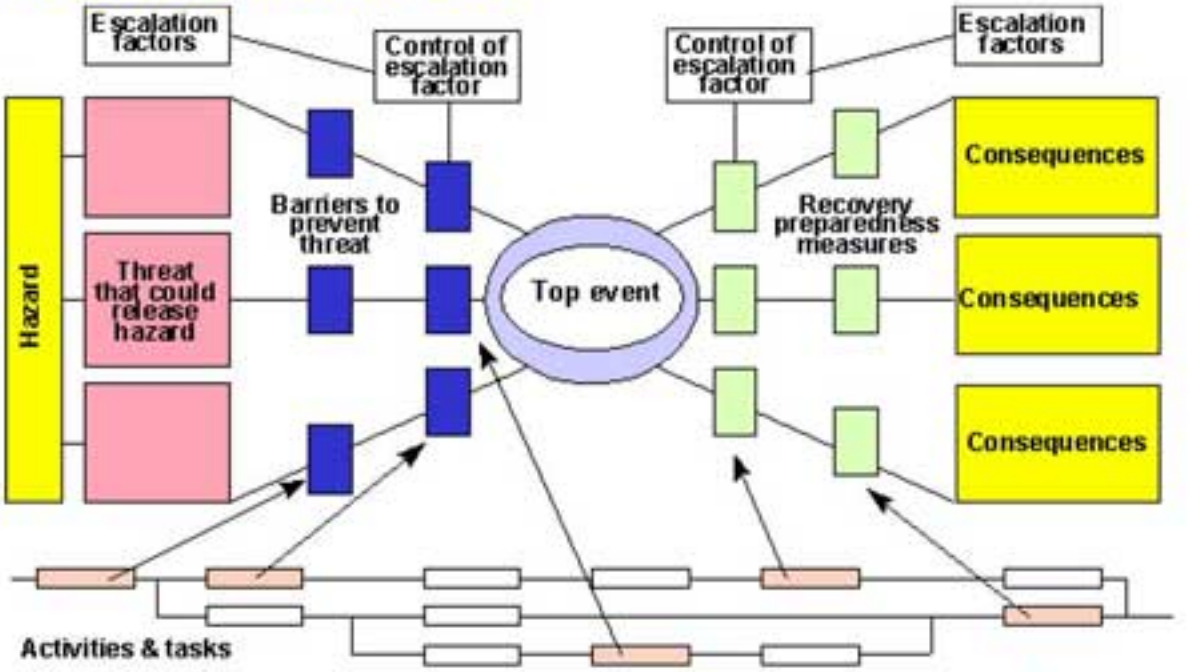
- Part 4 – **Description of Site:** To provide background to the risks and effects analysis and including, e.g., countermeasure systems and emergency, crisis management and business continuity plans.
- Part 5 – **Security Risk and Effects Register:** Shows that all security risks and effects are identified and evaluated. It defines the controls to manage the causes and consequences for significant risks.
- Part 6 – **Remedial Action Plan:** This summarises any shortfalls identified, with a plan to resolve the findings and thereby improve the security.
- Part 7 – **Statement of Fitness:** It explains that the risks and effects associated with the site have been evaluated and measures have been taken to reduce the risks to the lowest level that is reasonably practicable.

Protection:
Demonstrating Risk Mitigation – The Bow Tie Diagram

- Regulators and stakeholders worldwide expect more information to demonstrate that an operation/asset has an effective management system, showing that:
  - all credible **hazards** have been **identified**;
  - appropriate **standards** have been **set and met**;
  - adequate **security features** are **in place**;
  - all significant **assumptions** have been **identified, verified and validated**;
  - all **instructions, limits and conditions** required to maintain operations within specified margins for security **have been met**
- Several documents would be generated and fulfilling the requirements and the explanation of all the interactions between these documents becomes more difficult to explain to the workforce, regulator and stakeholders.

Protection:
Demonstrating Risk Mitigation – The Bow Tie Diagram

- Bow Tie diagram demonstrates how the security management system requirements are met with respect to the control and management of hazards and risks.
- Bow Ties depict the relationship between hazards, threats, barriers, escalation factors, controls, consequences, recovery preparedness measures and critical tasks



Conclusions

- A methodology to identify critical transport infrastructure is proposed
- Key parameters could be tuned to properly meet each case
- The instruments for its application at both government and specific asset manager levels exist
- Tools to demonstrate and properly handle security are available

D'APPOLONIA

Thank you for your attention