TACIT – Threat Assesment Framework for Critical Infraestructure Protection.

Simulation tool for Smart Grids Cyber Attacks

V Congreso Internacional de Seguridad Industrial (7/10/2015)

is an 18 months **collaborative CIPS project**

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Disclaimer: The information contained in this presentation reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Consortium

Project Coordinator

Is a private, non-profit, applied research center with strong market orientation through the innovation and technological development

Exploitation Manager

Is a division of ***everis*** *group that provides solutions for critical systems in aerospace, space, defense, security and emergency sectors.*

Validation Leader

Is a private large engineering consulting company with European relevance, really focused on critical sectors in the market

Dissemination Manager

Is one of the main independent organization for cyber security in Critical Infrastructures with relevance worldwide (as ex. in South Arabia, etc).

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Problems with SMART GRIDs

"*Networks of computers, intelligent electronic devices, software, and communication technologies* ***present greater infrastructure protection challenges than*** *those of the* ***traditional infrastructure****. Particularly, a smart grid includes more devices and connections that may become avenues for intrusions, error-caused disruptions, malicious attacks, destruction, and other threats* ***["Idaho National Laboratory"]****.*

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

SMART GRIDs: Most urgent attacks to protect from

TYPE OF ATTACKS

- DoS
- Firmware trusted
- Identity theft
- Password from the supplier
- Accountability and billing can be attacked
- Attack making use of the ICT solutions in place
- Attacks to physical assets
- Communication sniffing

ORDER OF PRIORITY

- First: DoS
- Second: Man in the middle/Sniff
- Third: Intrusion to the servers

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

TACIT project objectives

"TACIT will develop a **framework for the assessment** of risk and impact of **cyber attacks** in **smart grids** and **energy sectors**".

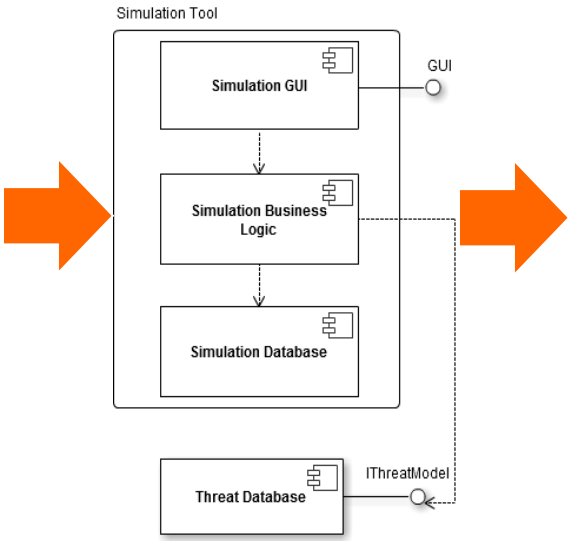
- Exchange of knowledge and experience, in order to establish best practices.
- The development of Critical Infrastructure (CI), in order to upgrade security in this very specific context, thanks to a real product that will be integrated over the CI, during TACIT execution.

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Methodology

Input

- Diagnosis current situation of cybersecurity in smartgrids
- Survey and workshop with relevant stakeholders and experts
- DB: Tecnalia's Threat model (based on OWASP risk rating methodology).
- Attack trees.



Validation

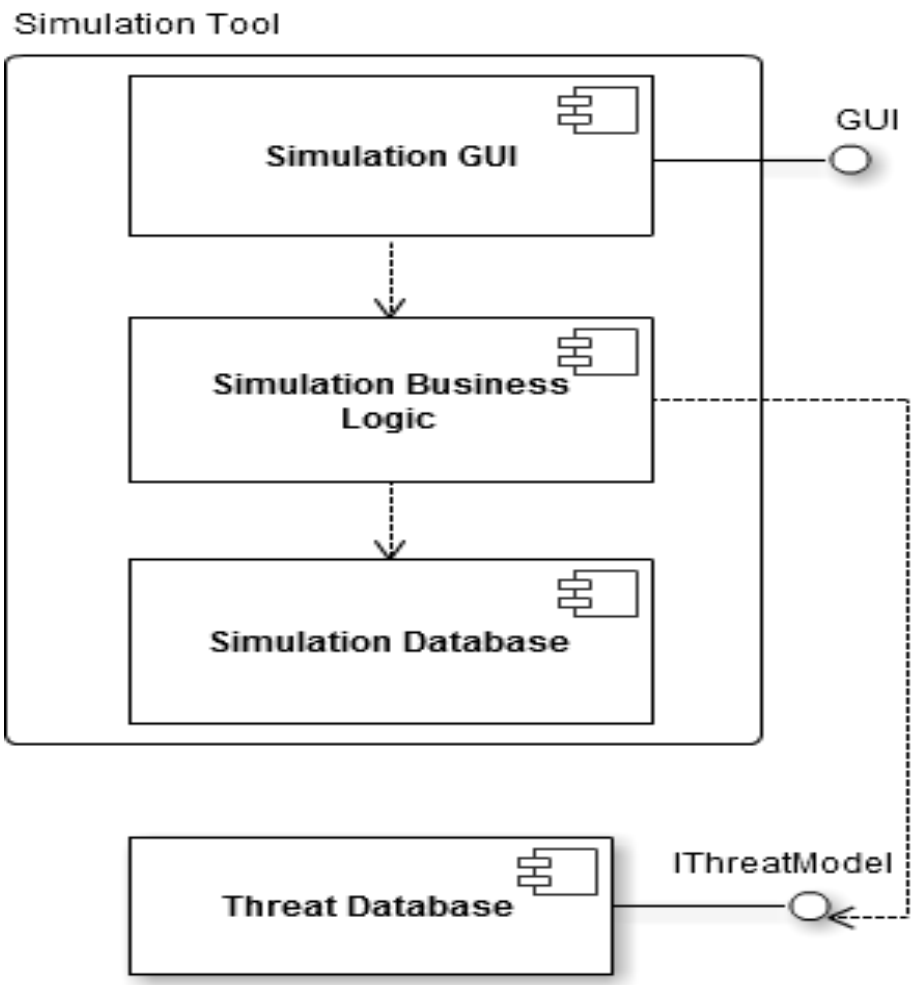
- **Effectiveness and usefulness tests** in a real electricity smartgrid laboratory (INGRID) of Tecnalia.
- **Usability and user acceptance tests** (external tests).

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

TACIT project main assets

SIMULATION TOOL

DATA BASE



Developed by **EVERIS**

Developed by **TECNALIA**

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Threats DataBase

Structured info on:

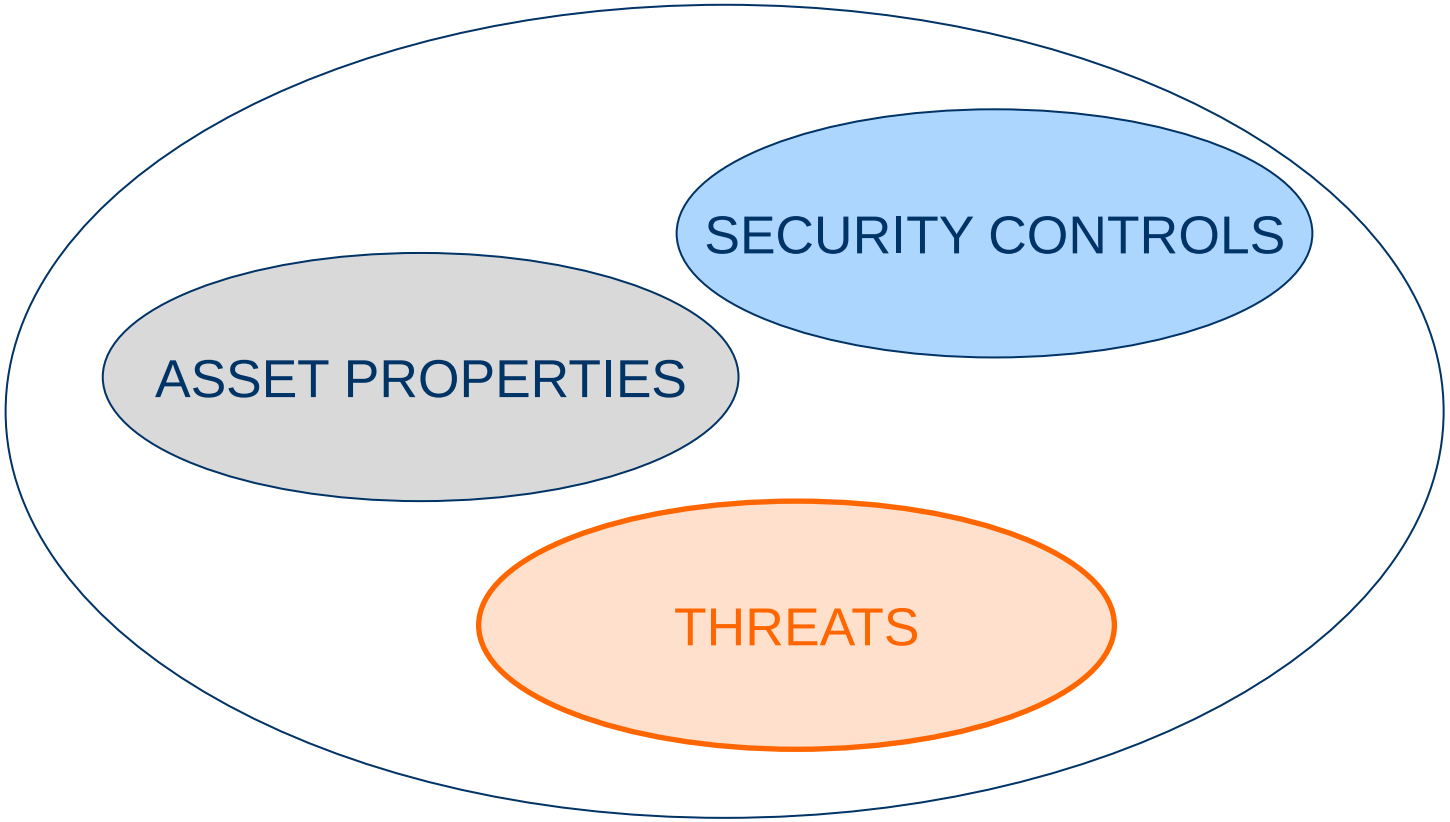
- Cyberattacks
- Vulnerabilities of the assets
- Security controls to prevent attacks
- Impact of attacks

per each SG component

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Understanding the simulation process (1/8)

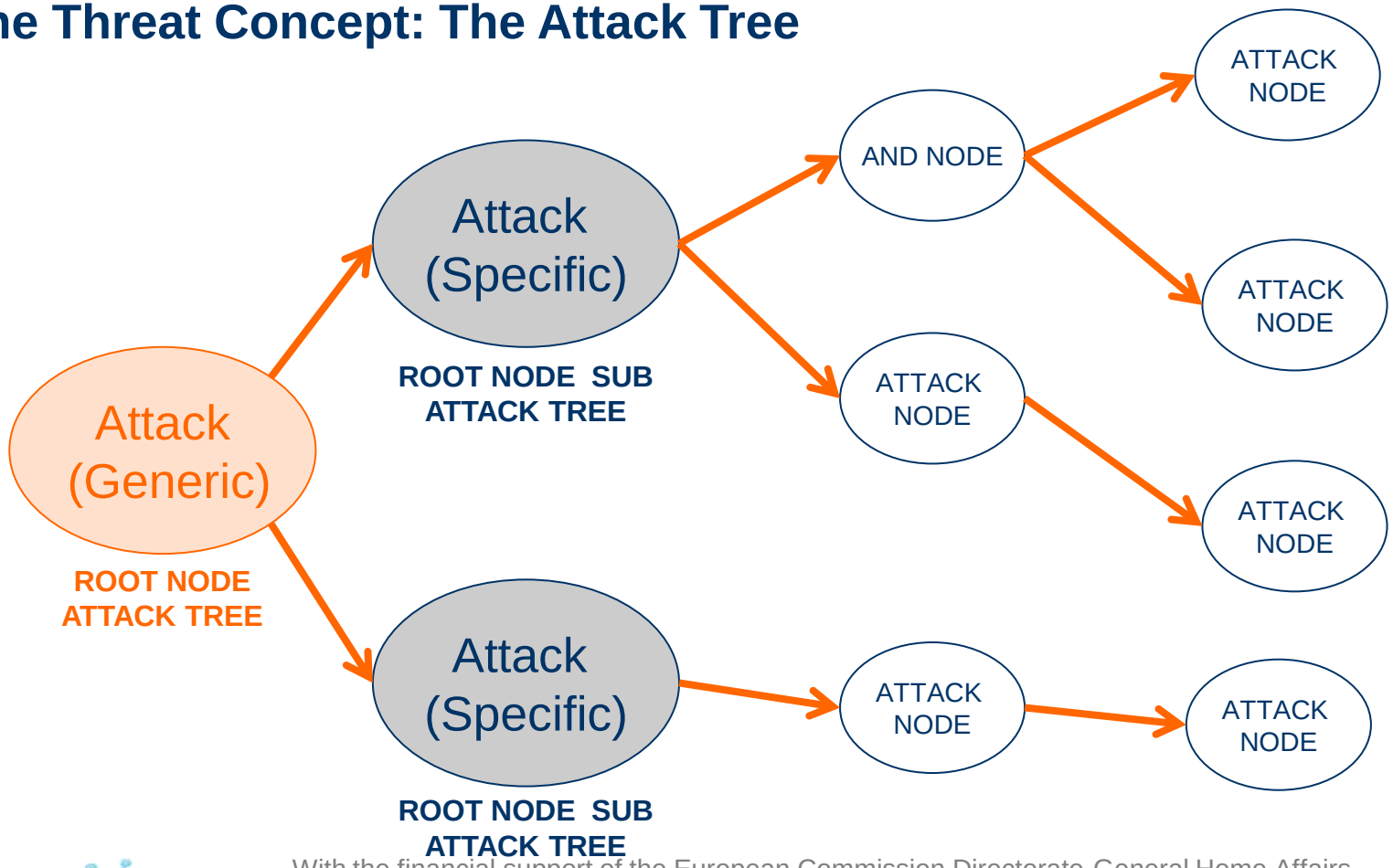
The Asset Concept



With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Understanding the simulation process (2/8)

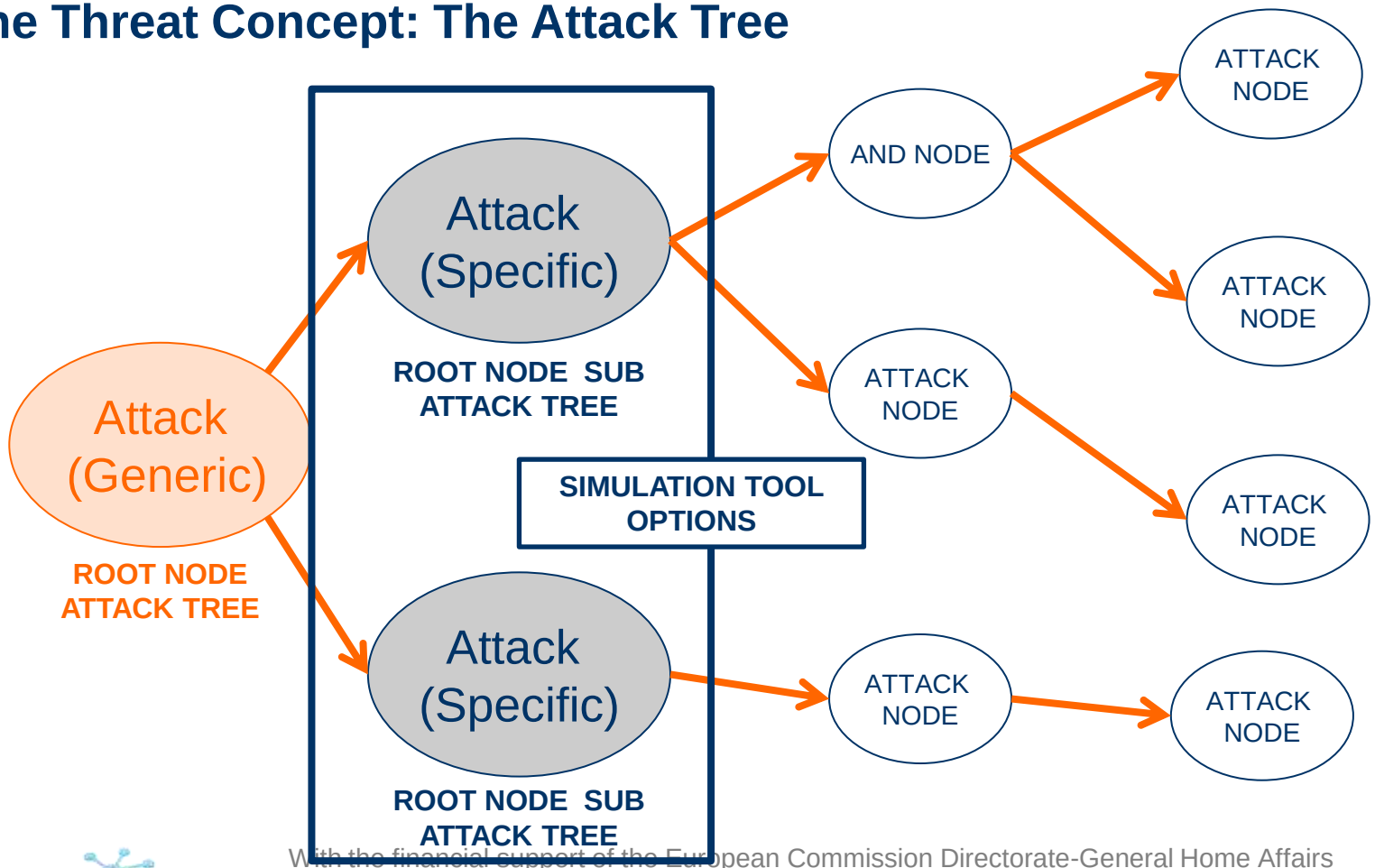
The Threat Concept: The Attack Tree



With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Understanding the simulation process (3/8)

The Threat Concept: The Attack Tree

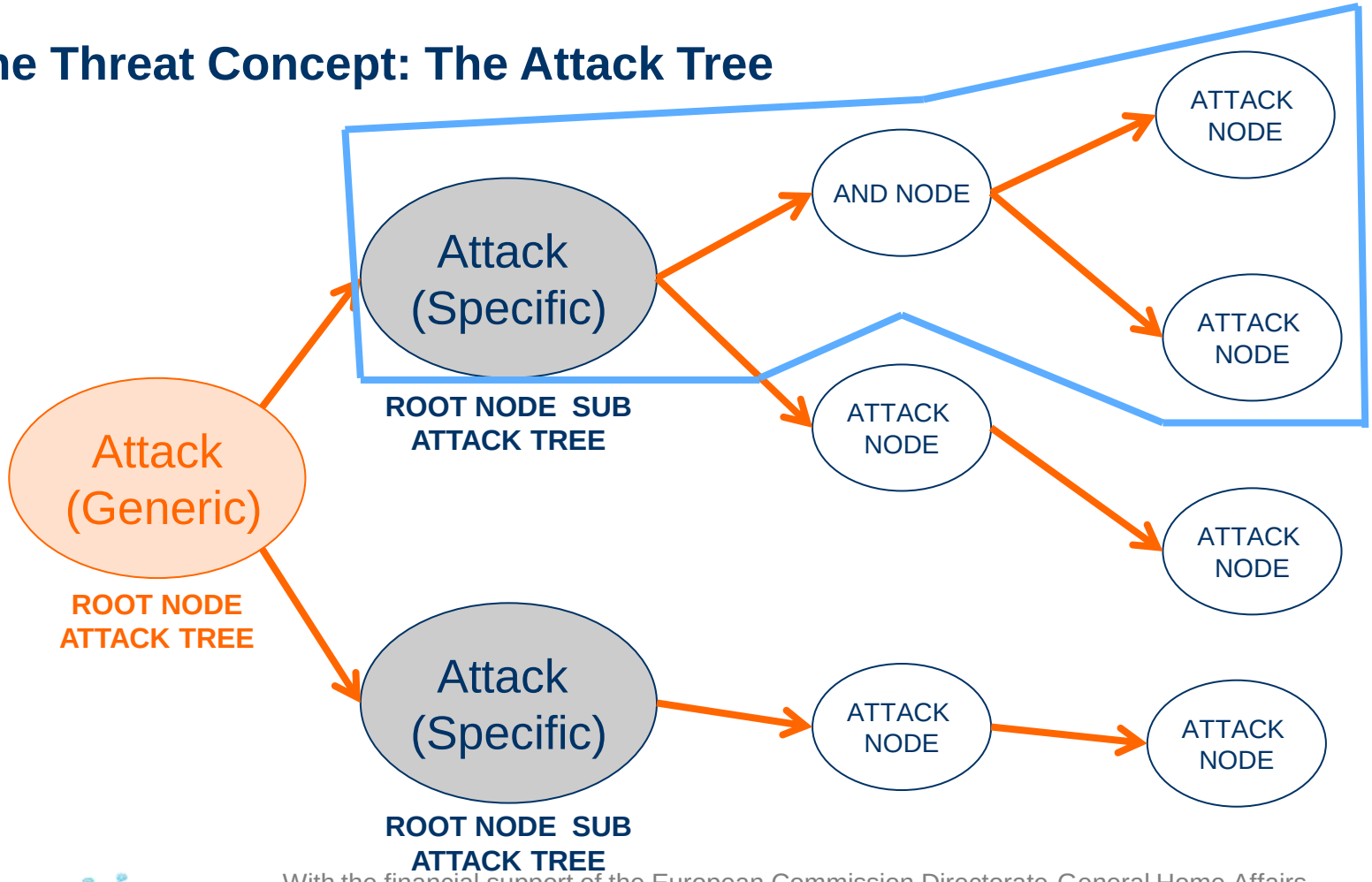


With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Understanding the simulation process (4/8)

ATTACK TREE BRANCH (ATTACK COMBINATION): 1

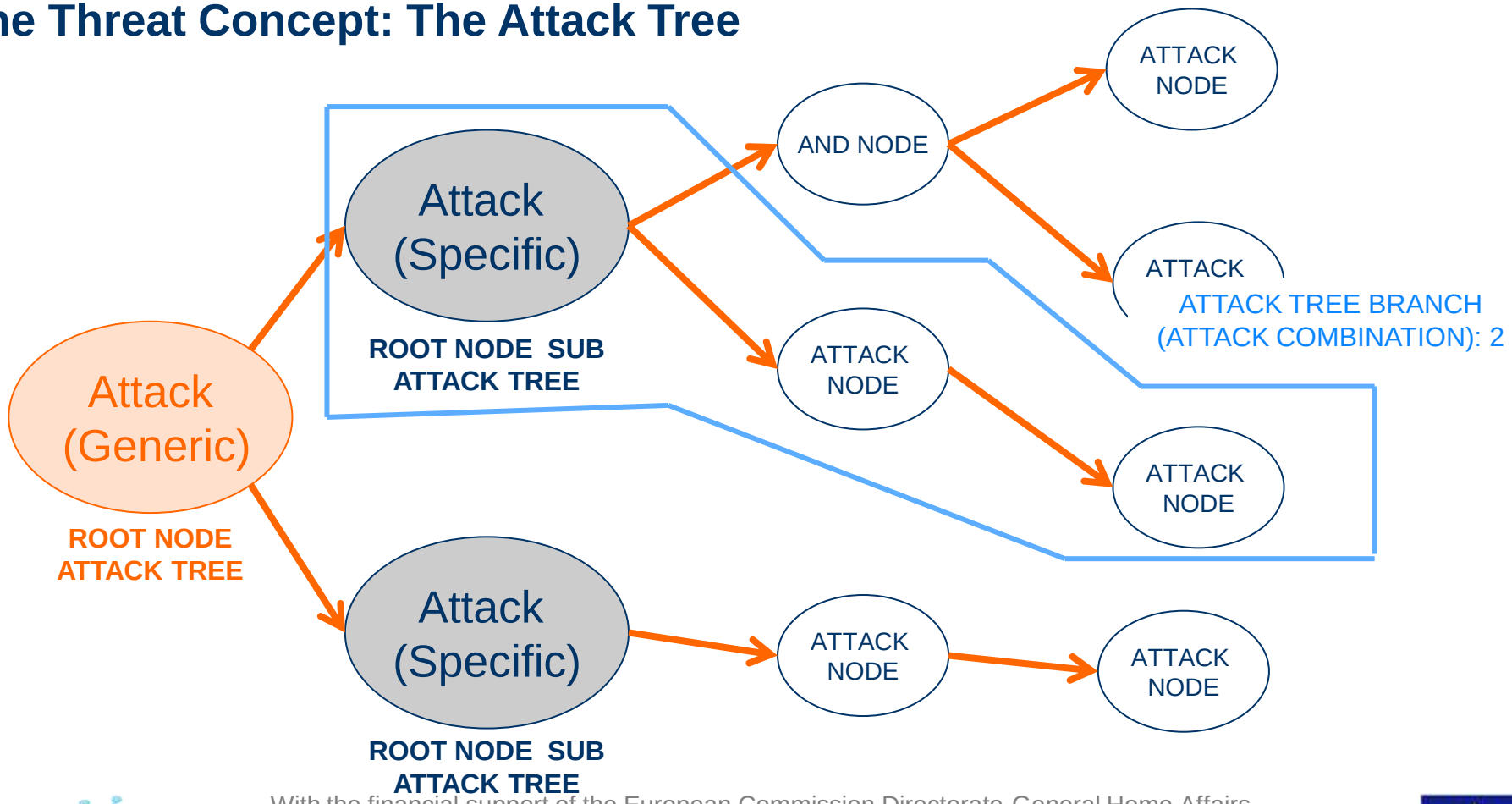
The Threat Concept: The Attack Tree



With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Understanding the simulation process (5/8)

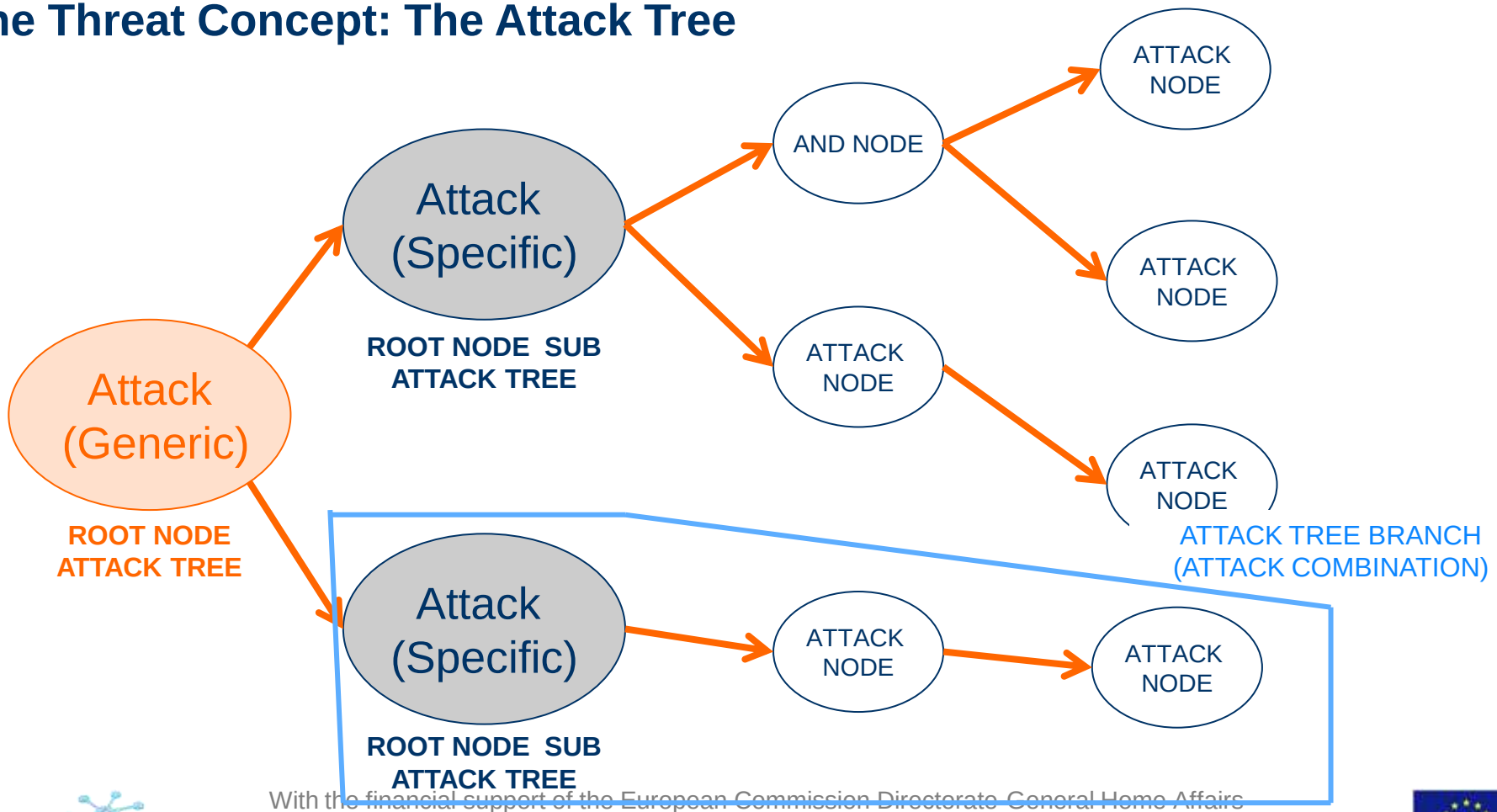
The Threat Concept: The Attack Tree



With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Understanding the simulation process (6/8)

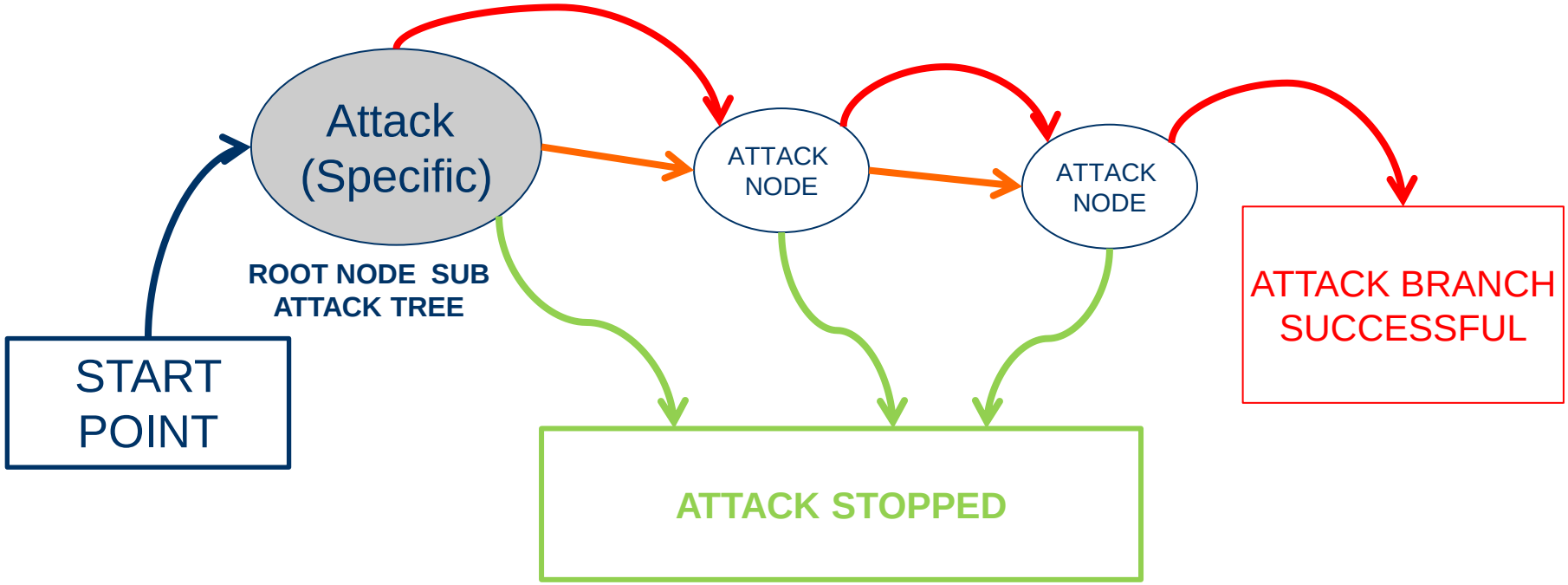
The Threat Concept: The Attack Tree



With the financial support of the European Commission Directorate General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Understanding the simulation process (7/8)

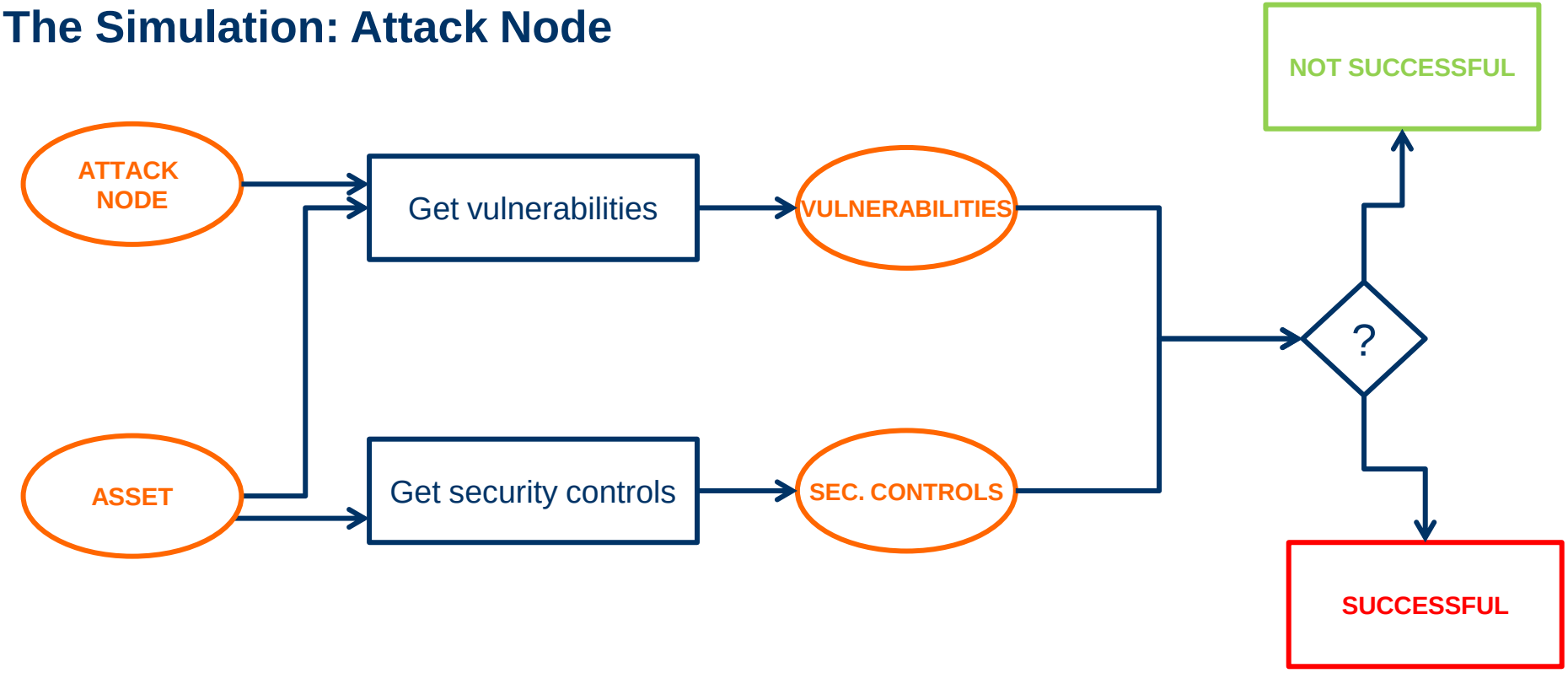
The Simulation:



With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Understanding the simulation process (8/8)

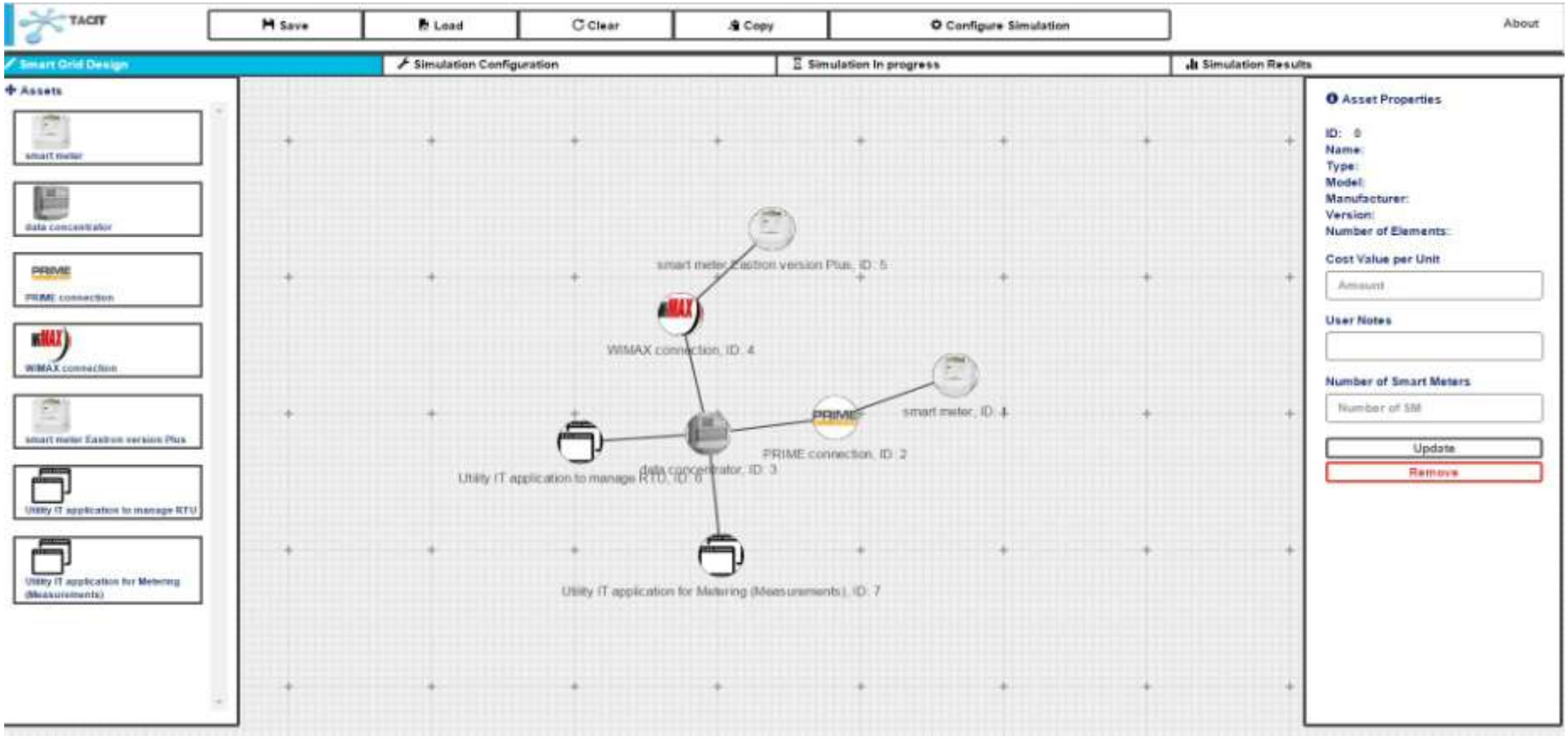
The Simulation: Attack Node



With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

How to simulate a cyber attack with TACIT simulation tool

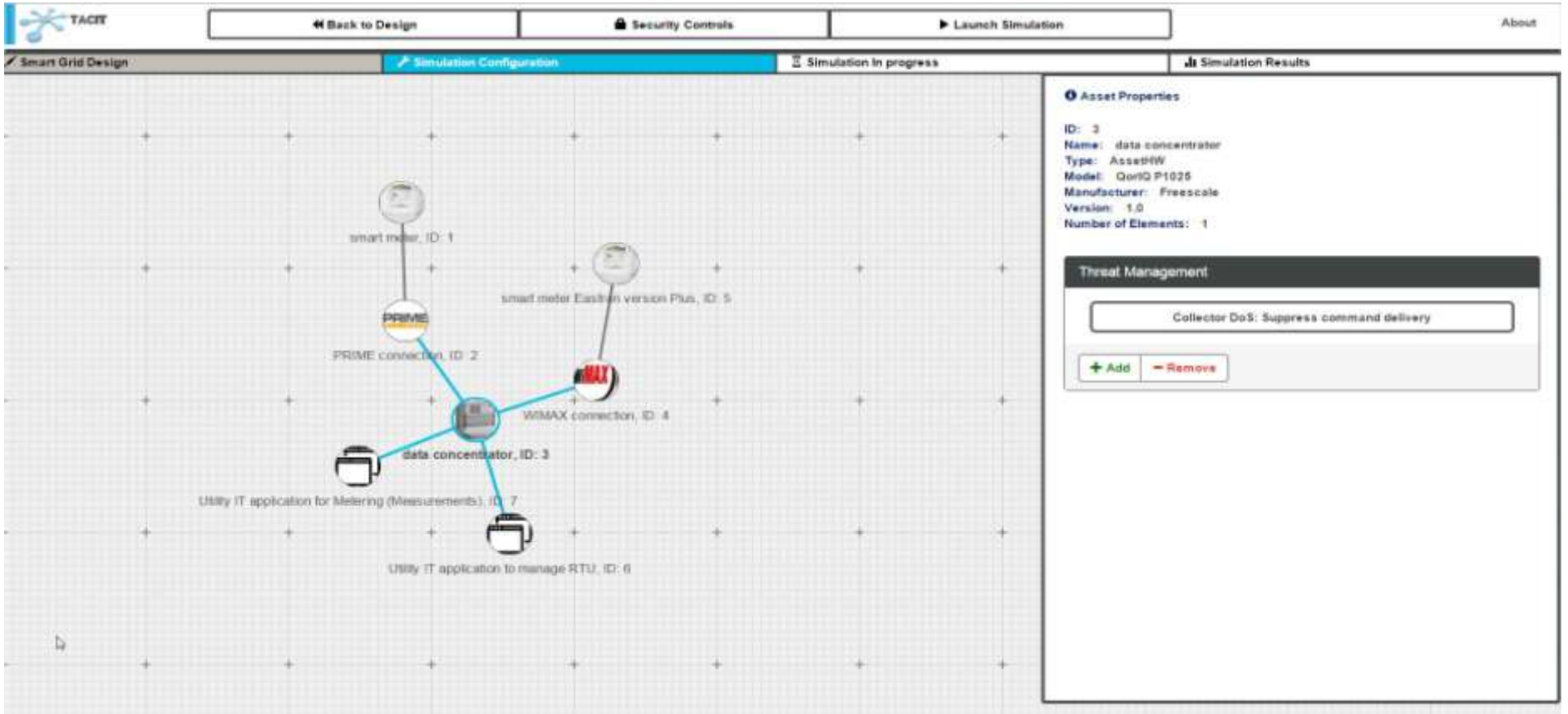
Step 1 – Design the SMART GRID



With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

How to simulate a cyber attack with TACIT simulation tool

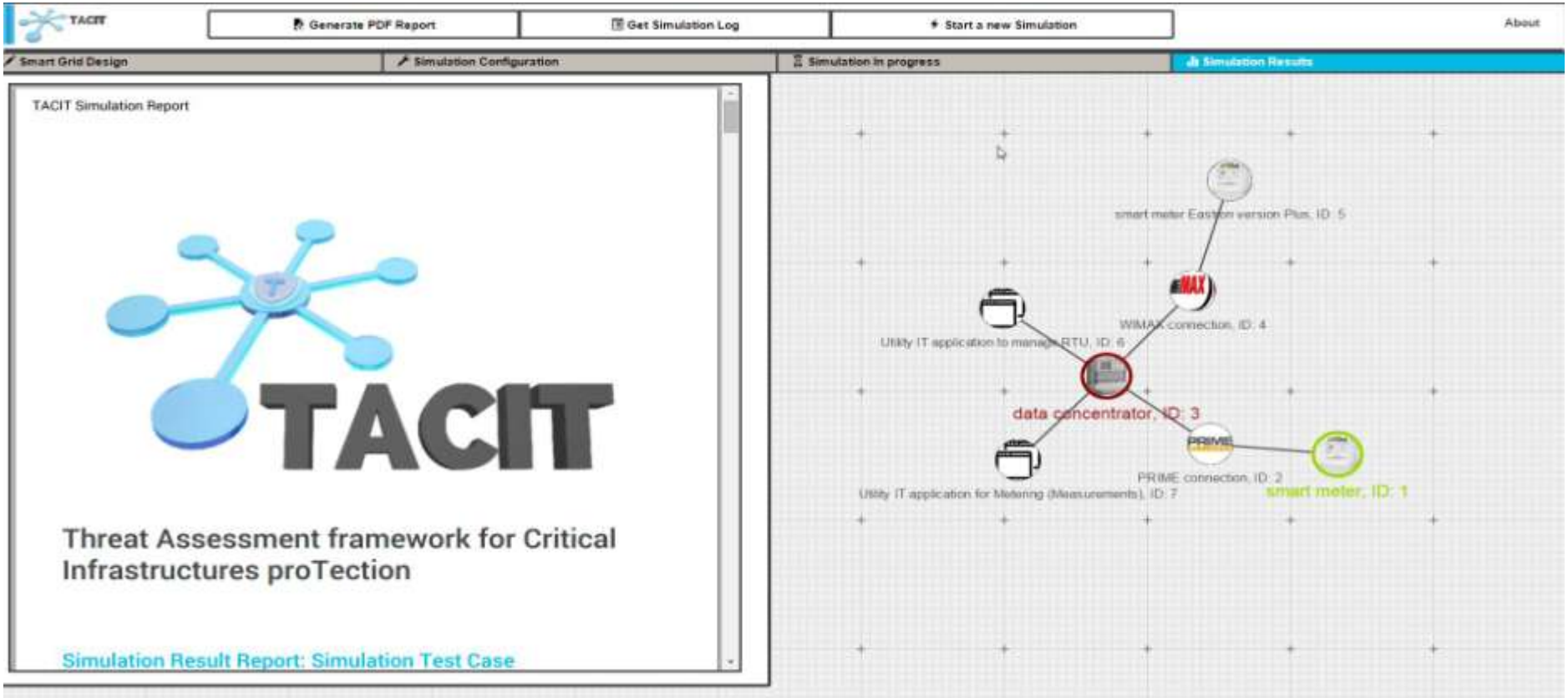
Step 2 – Configuration of cyber attacks



With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

How to simulate a cyber attack with TACIT simulation tool

Step 3 – Simulator results (1/2)



With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

How to simulate a cyber attack with TACIT simulation tool

Step 3 – Simulator results: Reports (2/2)

1. **Simulation Test Case Report:** Information about Smart Grid Configuration, Attack branches that are going to be used, and the attack nodes that make it up.

2. **Simulation Details Report:** Information about the attack branches' result, and for each attack node the vulnerabilities that it exploits and its result.

3. **Impact Report:** Technical and Business impacts for each exploited vulnerability.

4. **Recommendations Report:** The security control that could stop the attack in case of being applied for each compromised asset.

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Show video

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Target users of TACIT simulation tool

- **Smart Grid Designers**: learn how to address cybersecurity in the Smart Grid design.

- **Smart Grid Operators and technicians**: learn how to handle cyber-attacks and possible causes.

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Benefits of TACIT simulation tool

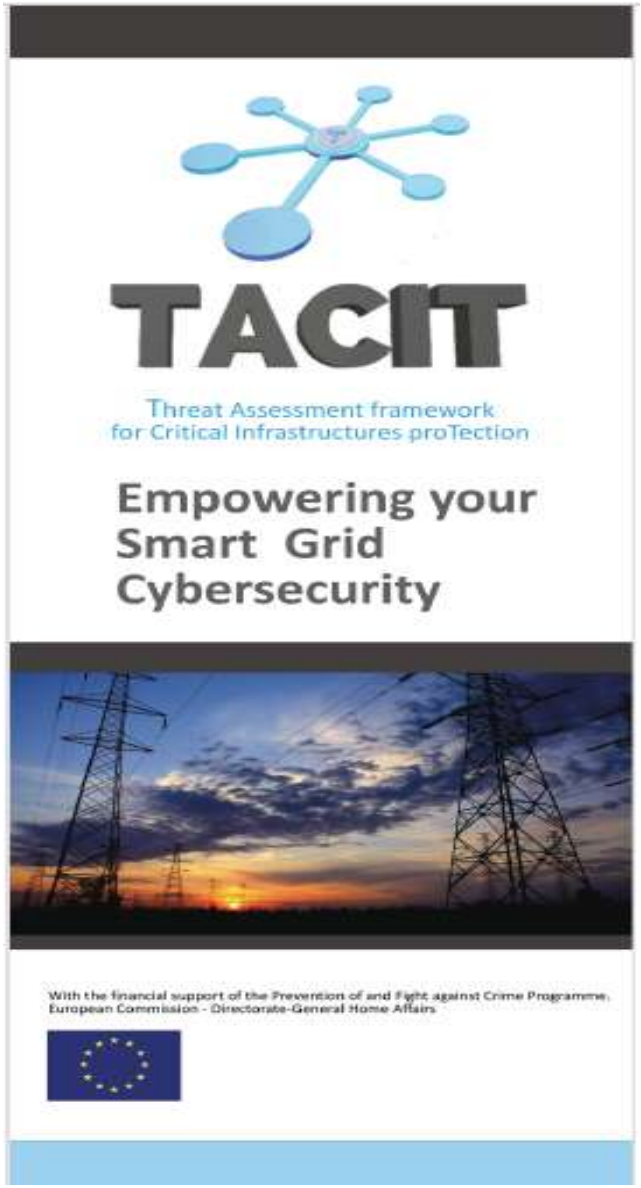
- Aid to design smart grids considering the security from the beginning.
- Ease the comprehension about security aspects of the smart grid for operators.
- A complement for audits without compromising the availability.
- An easy way to be up-to-date about vulnerabilities, how to protect them and impact of these vulnerabilities in the smart grid assets

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

Future challenges of TACIT tool

- Keep DB with **maintained up to date information on threats and security controls**.
- **Link** DB **to available public databases of threats and vulnerabilities**, e.g. Mitre's CVE, CWE, etc.
- Request companies to **populate DB** information **with knowledge on suffered attacks**. Public administration should help in maintaining the DB by pushing Information sharing among Companies.

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme



VISIT TACIT STAND FOR FURTHER INFORMATION

Conclusions

- TACIT provides a catalogue of attacks for electricity SMART GRIDs
- TACIT catalogue attacks can be extrapolated to other domains
- Simulation tools can be very useful in the design phase
- Provide information about risk and how to mitigate it
  - Select one device instead of another
  - Compare the numbers of countermeasures for a determined level of risk.
- Understanding the attack process

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

QUESTIONS?

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme

GRACIAS.

Jose Luis Díaz Rivera
Head of compliance – cybersecurity – everis
jdiazriv@everis.com

Alberto Domínguez
Experto en cyberseguridad – Smart Grids
adominguezs@everis.com

With the financial support of the European Commission Directorate-General Home Affairs Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme