



# **TACIT – Threat Assessment 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).*

# 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”**].*

# 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

# TACIT project objectives

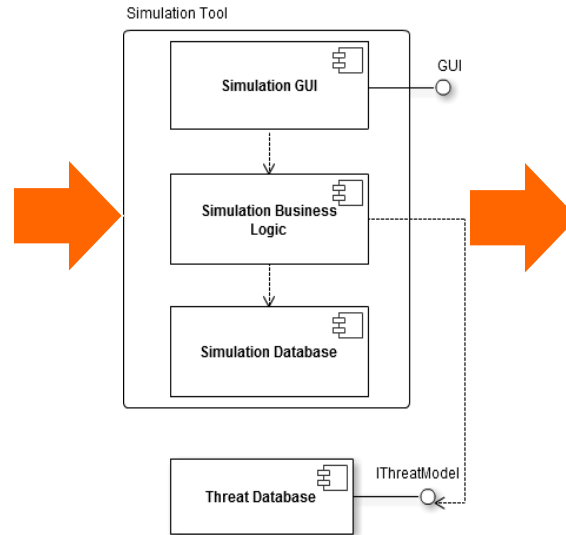
“TACIT will develop a **framework for the assessment** of risk and impact of **cyber attacks** in **smart grids** and **energy sectors**”.

- 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.

# Methodology

## Input

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



## Validation

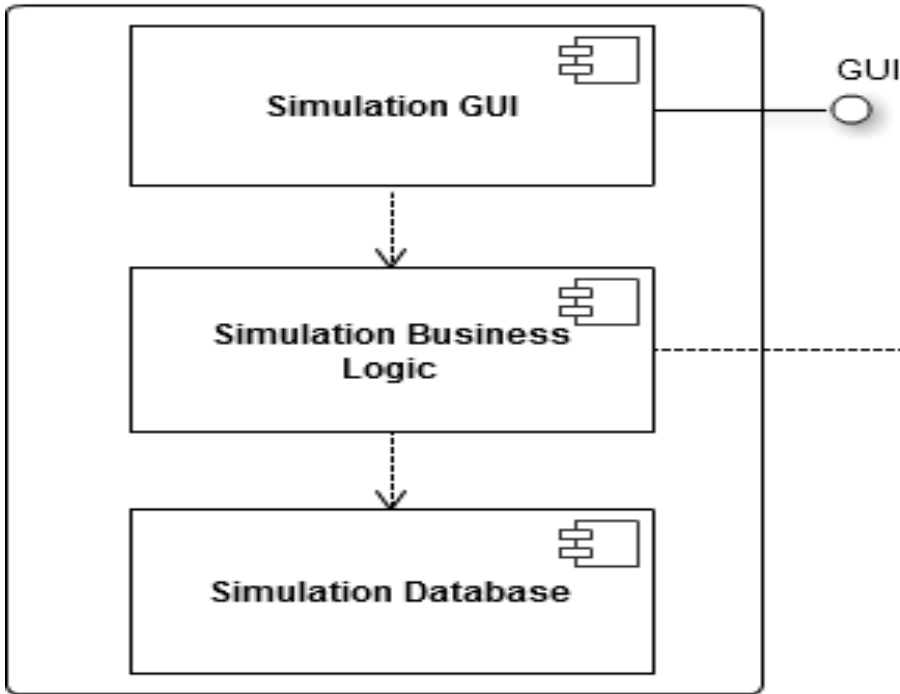
- **Effectiveness and usefulness tests** in a real electricity smartgrid laboratory (INGRID) of Tecnia.
- **Usability and user acceptance tests** (external tests).

# TACIT project main assets

SIMULATION TOOL

DATA BASE

Simulation Tool



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:

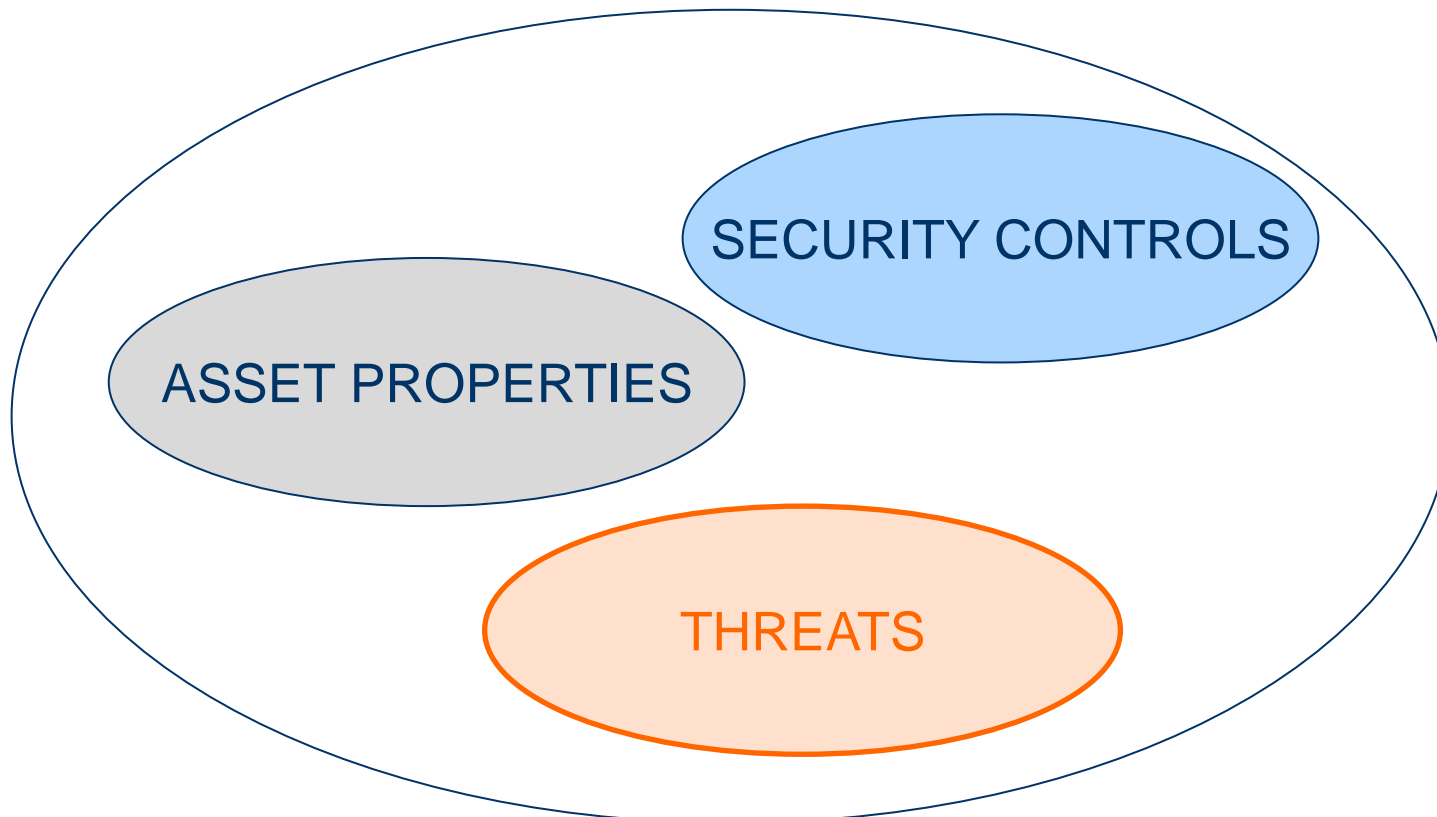
- Cyberattacks
- Vulnerabilities of the assets
- Security controls to prevent attacks
- Impact of attacks



**per each SG component**

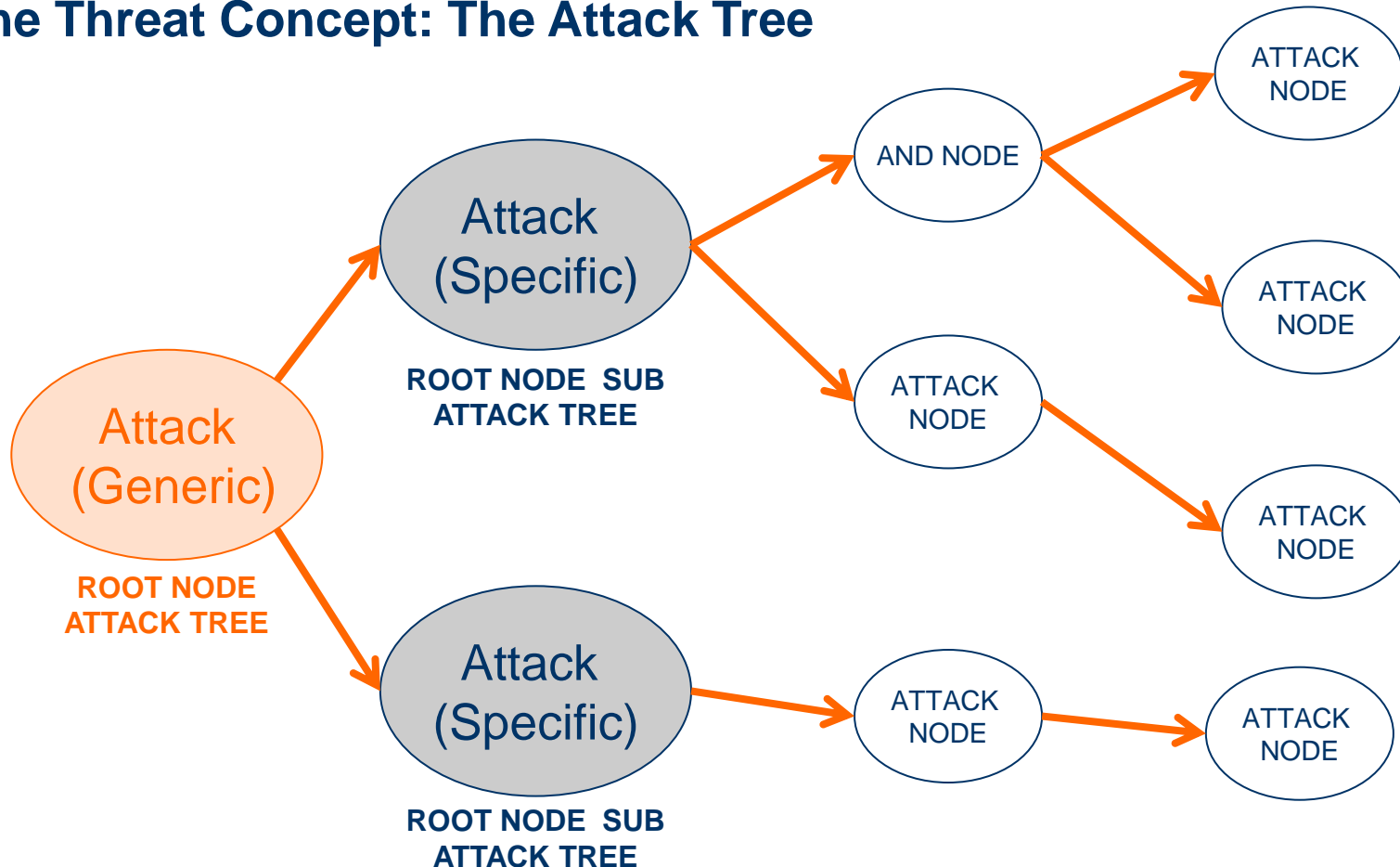
# Understanding the simulation process (1/8)

## The Asset Concept



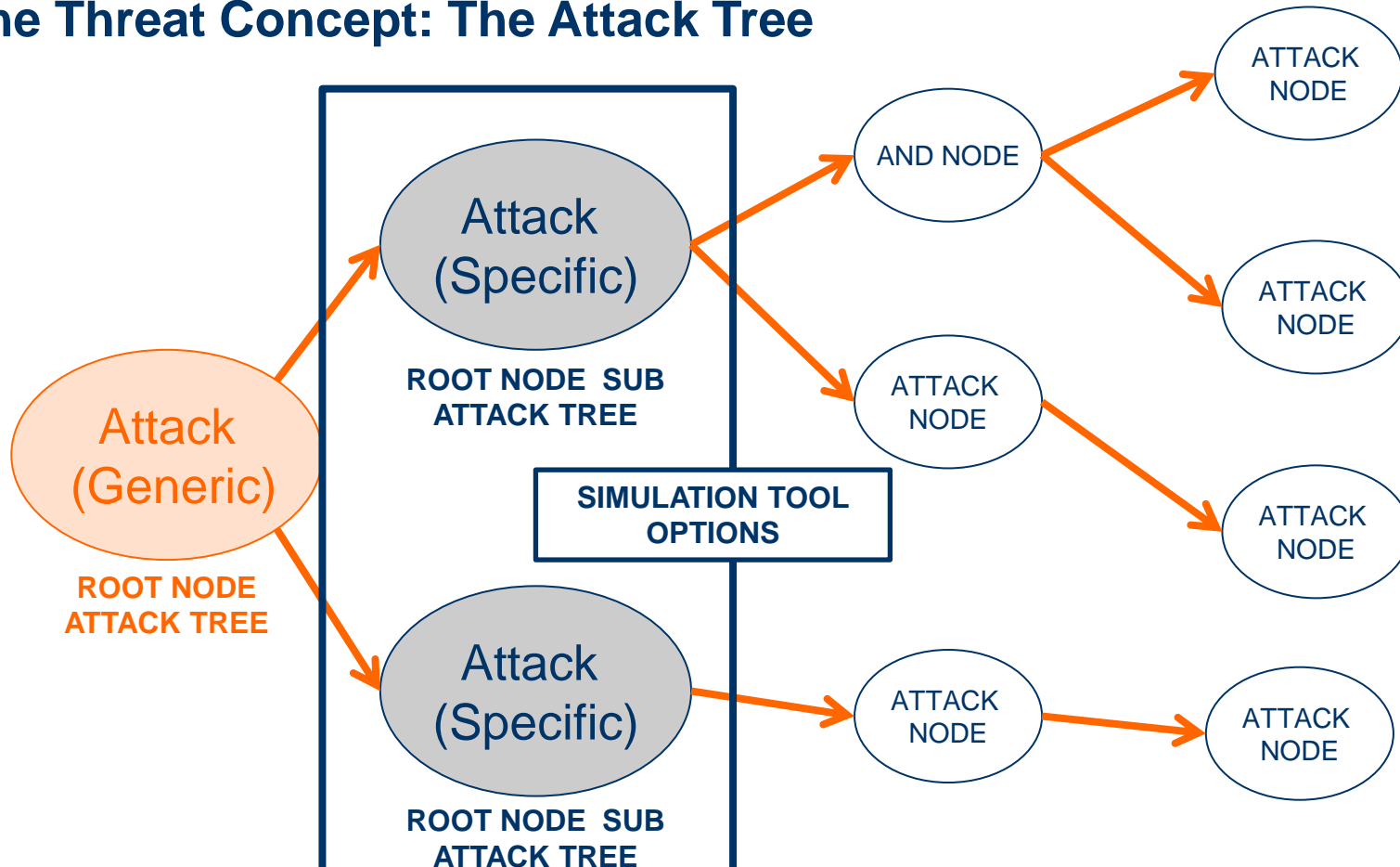
# Understanding the simulation process (2/8)

## The Threat Concept: The Attack Tree



# Understanding the simulation process (3/8)

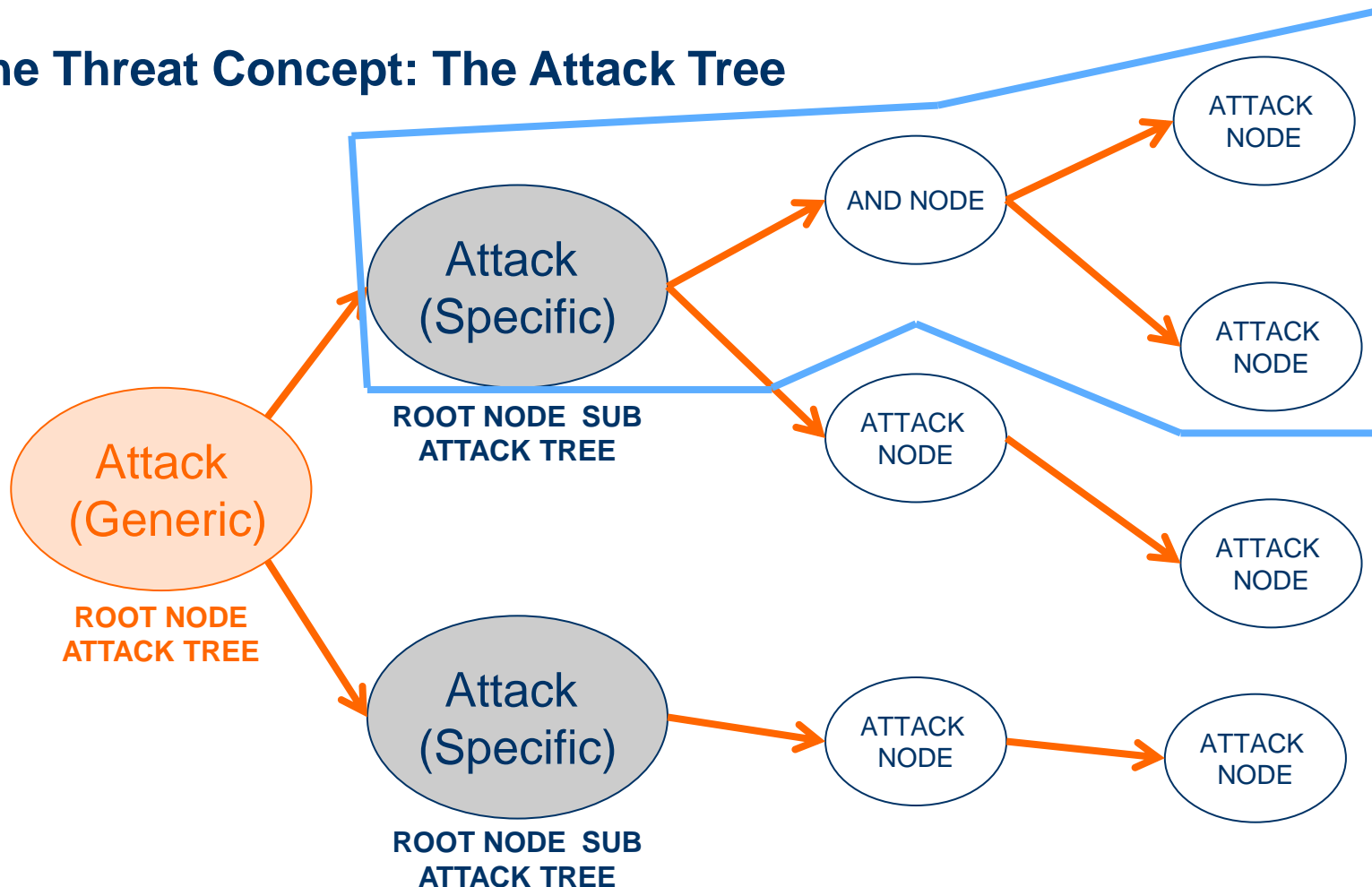
## The Threat Concept: The Attack Tree



# Understanding the simulation process (4/8)

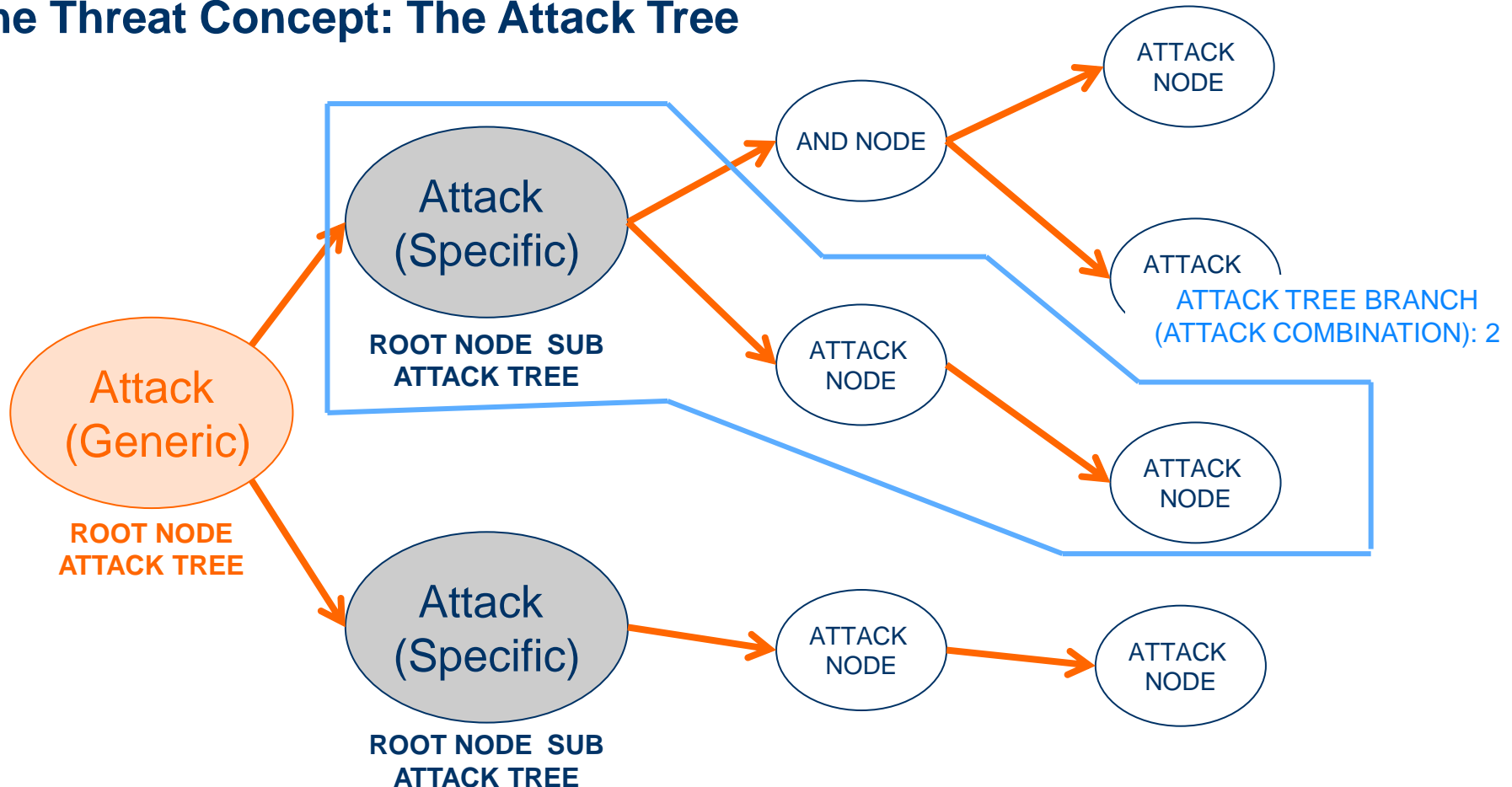
ATTACK TREE BRANCH  
(ATTACK COMBINATION): 1

## The Threat Concept: The Attack Tree



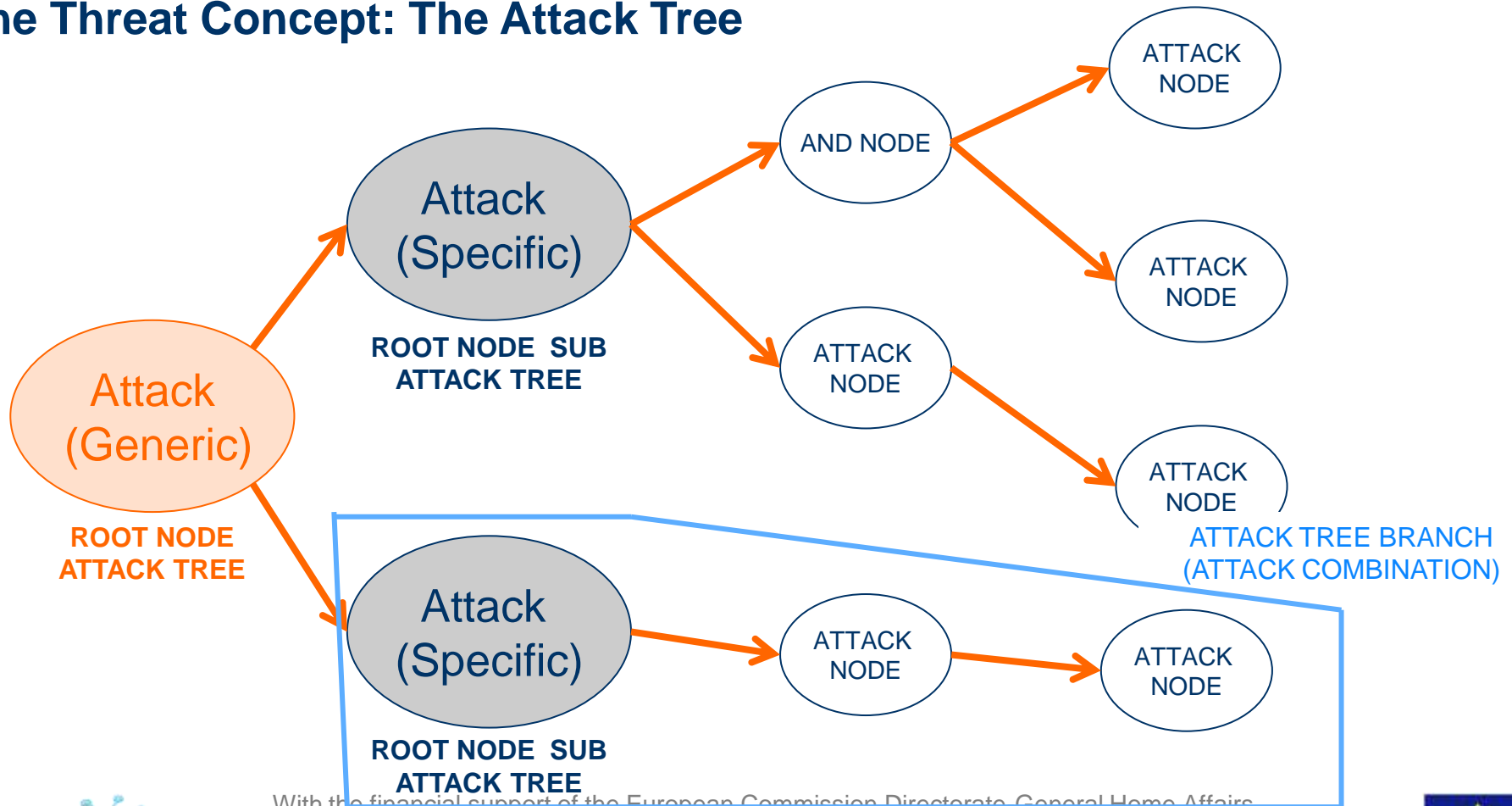
# Understanding the simulation process (5/8)

## The Threat Concept: The Attack Tree



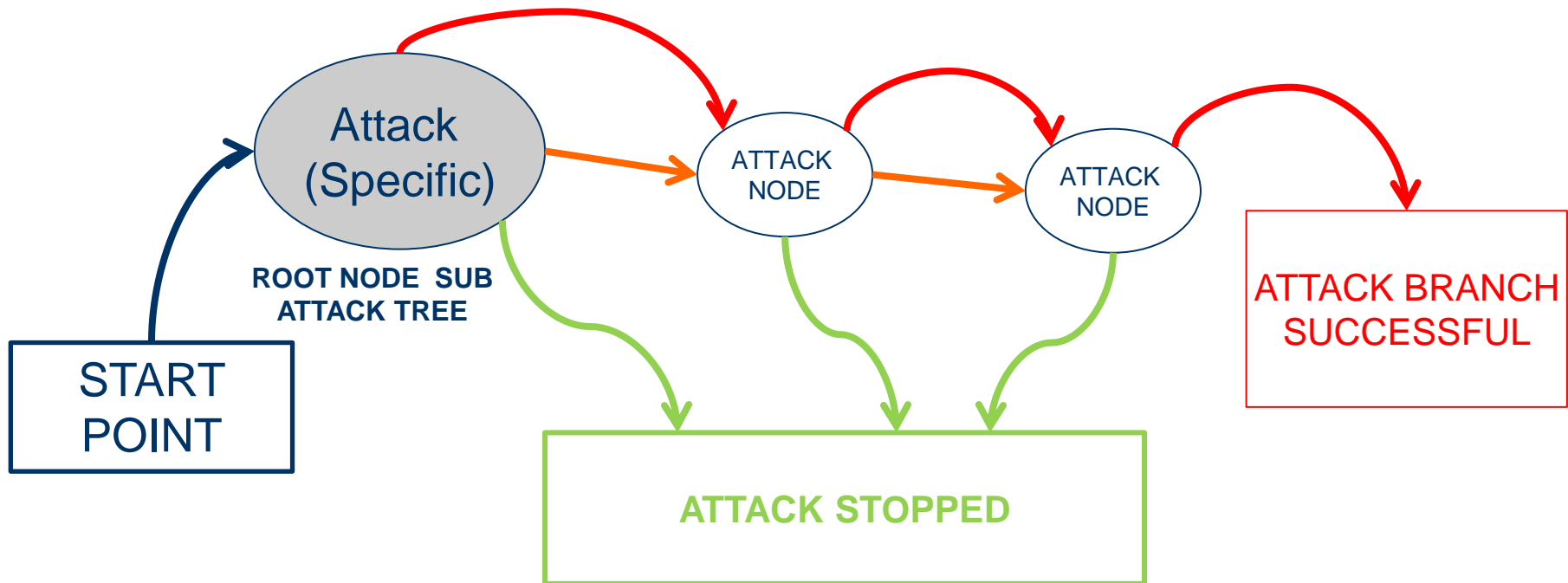
# Understanding the simulation process (6/8)

## The Threat Concept: The Attack Tree



# Understanding the simulation process (7/8)

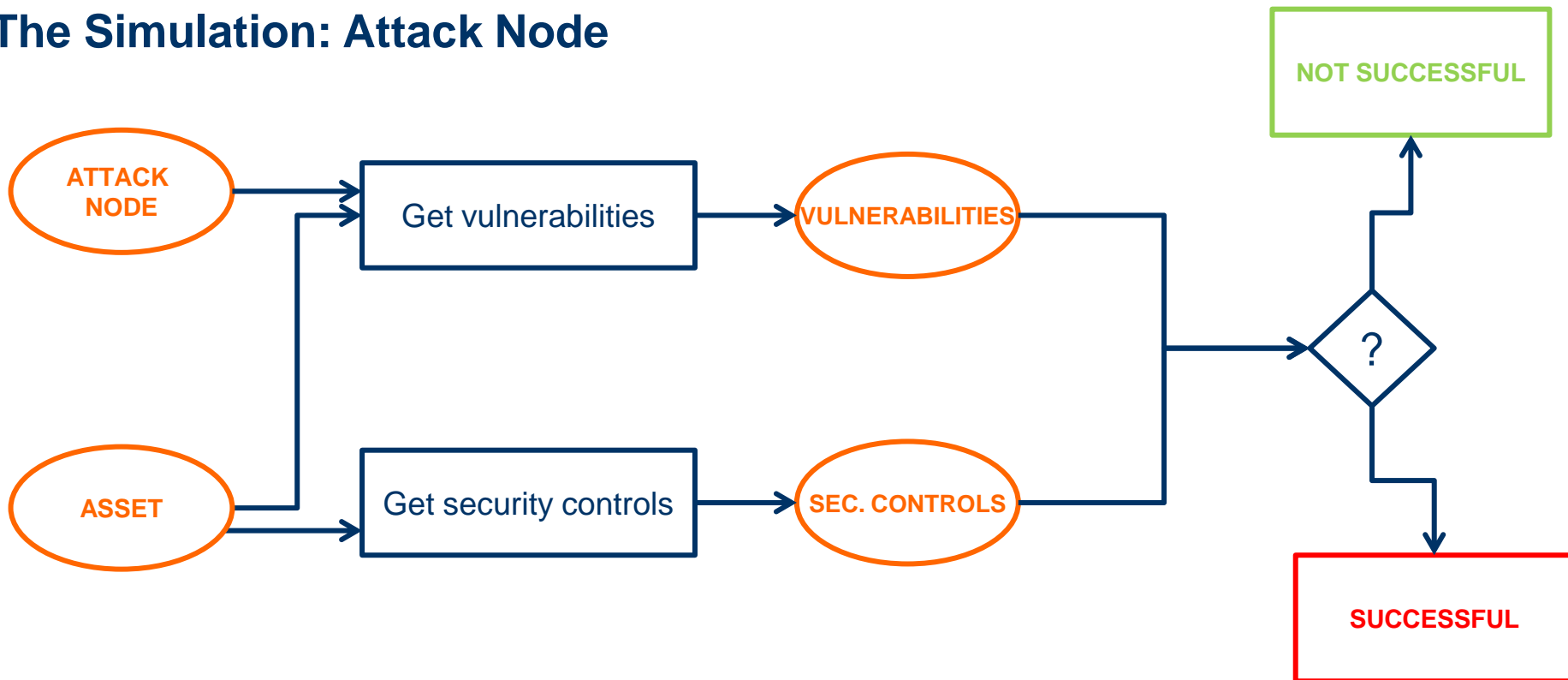
## The Simulation:





# Understanding the simulation process (8/8)

## The Simulation: Attack Node



# How to simulate a cyber attack with TACIT simulation tool

## Step 1 – Design the SMART GRID

The screenshot displays the TACIT simulation tool interface. At the top, there is a menu bar with options: Save, Load, Clear, Copy, and Configure Simulation. Below the menu bar, the main workspace is divided into three tabs: Smart Grid Design (active), Simulation Configuration, Simulation In progress, and Simulation Results. On the left side, there is an 'Assets' panel with a list of components: smart meter, data concentrator, PRIME connection, WMAX connection, smart meter Easlon version Plus, Utility IT application to manage RTU, and Utility IT application for Metering (Measurements). The central workspace shows a network diagram with a central 'data concentrator, ID: 3' connected to several other components: 'Utility IT application to manage RTU, ID: 6', 'Utility IT application for Metering (Measurements), ID: 7', 'WMAX connection, ID: 4', 'PRIME connection, ID: 2', and 'smart meter, ID: 5'. The 'smart meter, ID: 5' is further connected to 'smart meter Easlon version Plus, ID: 6'. On the right side, there is an 'Asset Properties' panel with fields for ID, Name, Type, Model, Manufacturer, Version, and Number of Elements. It also includes a 'Cost Value per Unit' section with an 'Amount' input field, a 'User Notes' section with a text area, and a 'Number of Smart Meters' section with a 'Number of SM' input field. At the bottom of the panel are 'Update' and 'Remove' buttons.

# How to simulate a cyber attack with TACIT simulation tool

## Step 2 – Configuration of cyber attacks

The screenshot displays the TACIT simulation tool interface. At the top, there is a navigation bar with buttons for "Back to Design", "Security Controls", and "Launch Simulation". Below this is a secondary navigation bar with tabs for "Smart Grid Design", "Simulation Configuration" (which is active), "Simulation In progress", and "Simulation Results".

The main workspace shows a network diagram on a grid background. The diagram includes several nodes and connections:

- smart meter, ID: 1
- PRIME connection, ID: 2
- smart meter Easton version Plus, ID: 5
- WIMAX connection, ID: 4
- data concentrator, ID: 3
- Utility IT application for Metering (Measurements), ID: 7
- Utility IT application to manage RTU, ID: 6

On the right side, there is a panel titled "Asset Properties" for the selected "data concentrator" (ID: 3). The properties listed are:

- Name: data concentrator
- Type: AssetFW
- Model: QorIQ P1026
- Manufacturer: Freescale
- Version: 1.0
- Number of Elements: 1

Below the asset properties is a "Threat Management" section. It contains a text input field with the value "Collector DoS: Suppress command delivery". Below the input field are two buttons: "+ Add" and "- Remove".

# How to simulate a cyber attack with TACIT simulation tool

## Step 3 – Simulator results (1/2)

The screenshot displays the TACIT simulation tool interface. The top navigation bar includes the TACIT logo, buttons for 'Generate PDF Report', 'Get Simulation Log', and 'Start a new Simulation', and an 'About' link. Below this, a secondary navigation bar shows 'Smart Grid Design', 'Simulation Configuration', 'Simulation in progress', and 'Simulation Results' (which is highlighted in blue). The main content area is split into two panels. The left panel, titled 'TACIT Simulation Report', features the TACIT logo and the text 'Threat Assessment framework for Critical Infrastructures proTection'. At the bottom of this panel, it reads 'Simulation Result Report: Simulation Test Case'. The right panel displays a network diagram on a grid background. The diagram shows a central node labeled 'data concentrator, ID: 3' connected to several other nodes: 'smart meter Eastern version Plus, ID: 5' (top), 'WIMAX connection, ID: 4' (right), 'PRIME connection, ID: 2' (bottom right), 'smart meter, ID: 1' (bottom right), 'Utility IT application for Metering (Measurements), ID: 7' (bottom left), and 'Utility IT application to manage RTU, ID: 6' (left). A mouse cursor is visible over the diagram.

# 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.

# 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.

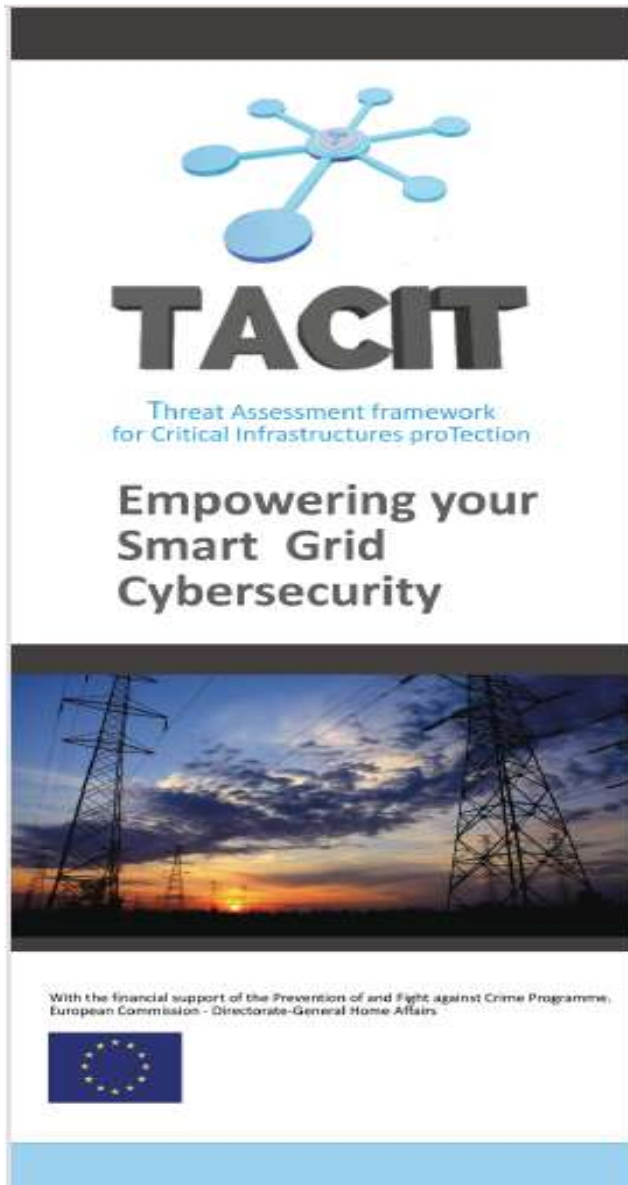
# Benefits of TACIT simulation tool

- 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



# 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.



**VISIT TACIT STAND FOR FURTHER INFORMATION**



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



# 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

# QUESTIONS?



# GRACIAS.

**Jose Luis Díaz Rivera**

Head of compliance – cybersecurity – everis

[jdiazriv@everis.com](mailto:jdiazriv@everis.com)

**Alberto Domínguez**

Experto en ciberseguridad – Smart Grids

[adominguezs@everis.com](mailto:adominguezs@everis.com)