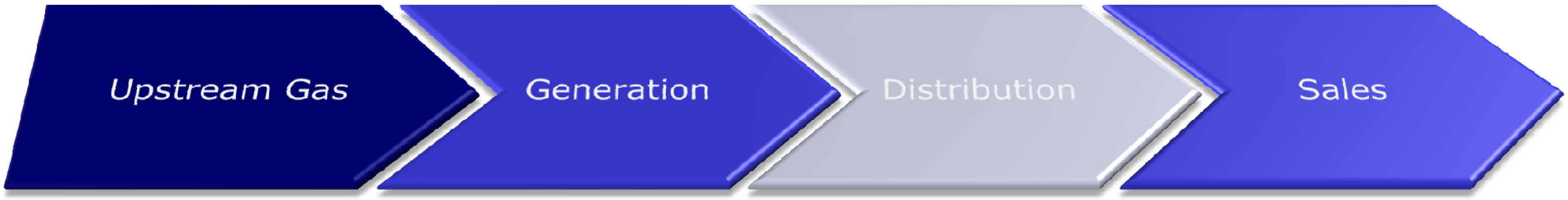
Physical Security in Enel within Italy Area

Ing. Gaetano Condorelli
Head of Infrastructure Security and Crisis Management

ERNCIP Meeting
30 October 2013
Genova

Enel overview

Integrated energy player



73,700 Employees

1.33 Mln shareholders

Serving the communities

16.7 Bln € EBITDA

97.800 Installed MW

61 Mln customers

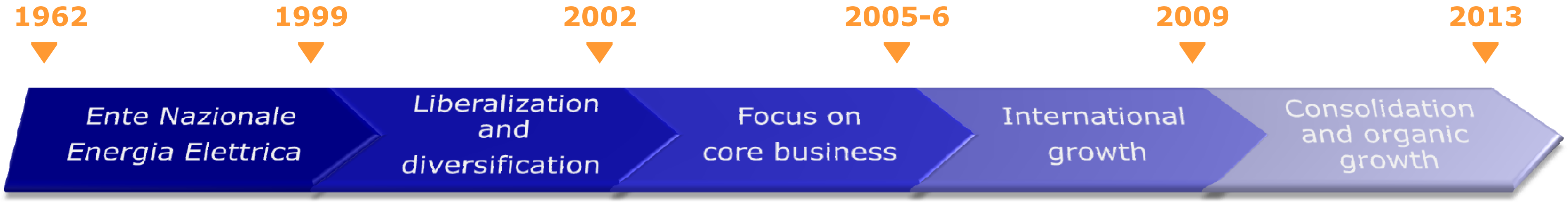
Security

Respect of environment

Creates and distributes value in the international energy market

Enel overview

Enel's transformation milestones



1962

1999

2002

2005-6

2009

2013

Ente Nazionale Energia Elettrica

Liberalization and diversification

Focus on core business

International growth

Consolidation and organic growth

- 1962: **Nationalization** of 1,300 energy companies
- 1987: **Nuclear power generation banned** in Italy
- 1992: Privatization of Enel SpA

- 1999: **Liberalization** of the electricity sector (Bersani Decree)
- 1999: Unbundling and incorporation of the **ISO** (GRTN)
- 1999: **Enel's IPO** (Milan, NYSE)
- Diversification in non-core business (**multiutility** model)
- 2002: **GenCos** and Distribution assets disposal

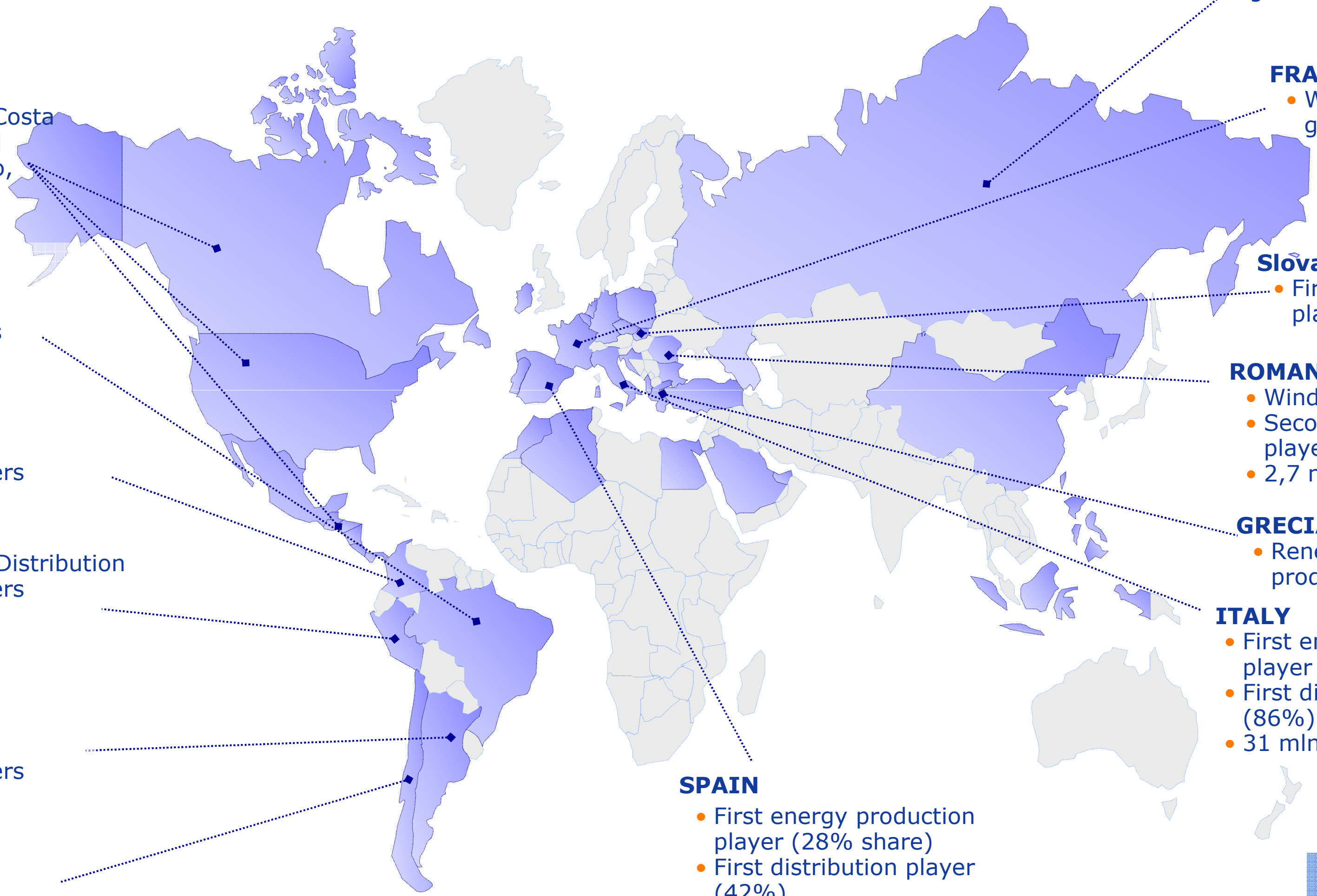
- 2004: **Disposal of non-core assets** (Enel Hydro, Real Estate…)
- 2004: **Terna's IPO**
- 2005: **Disposal of additional Enel's stake in Terna**, which acquires GRTN (from ISO to TSO)
- 2005: Divestiture of WIND

- 2005: **Acquisitions** of Slovenské Elektrarne (**Slovakia**) and Distribution Companies in **Rumania**
- 2006: Acquisition of RusEnergoSbyt (Russia)
- 2007: **Endesa's Public Purchase Offer** (Iberia and Latin America)
- 2008: Acquisition of OGK-5 and Severnergia (Russia)
- 2009: Complete acquisition of Endesa (Iberia ed Latin America)

- 2009-2011: Disposal of non-core assets (Maritza III East, Distribution grids for gas, HV grids in Spain); upstream gas activities
- 2010: EGP's IPO
- 2011: **Nuclear power generation banned** in Italy
- 2012: **Disposal of residual** Enel's stake in Terna
- 2011-2013: Strengthen company perimeter

Enel overview

Main country presence



NORTH-CENTER AMERICA
- North America, Costa Rica, Panama, El Salvador, Mexico, Guatemala

BRAZIL
- Generation and Distribution
- 6 mln customers

COLOMBIA
- Generation and Distribution
- 2,8 mln customers

PERU
- Generation and Distribution
- 1,2 mln customers

ARGENTINA
- Generation and Distribution
- 2,4 mln customers

CHILE
- Generation and Distribution
- 1,7 mln customers

SPAIN
- First energy production player (28% share)
- First distribution player (42%)
- 13 mln customers

RUSSIA
- First integrated energy player (upstream, generation, sales)

FRANCE
- Wind energy generation

Slovakia
- First energy productio player (78%)

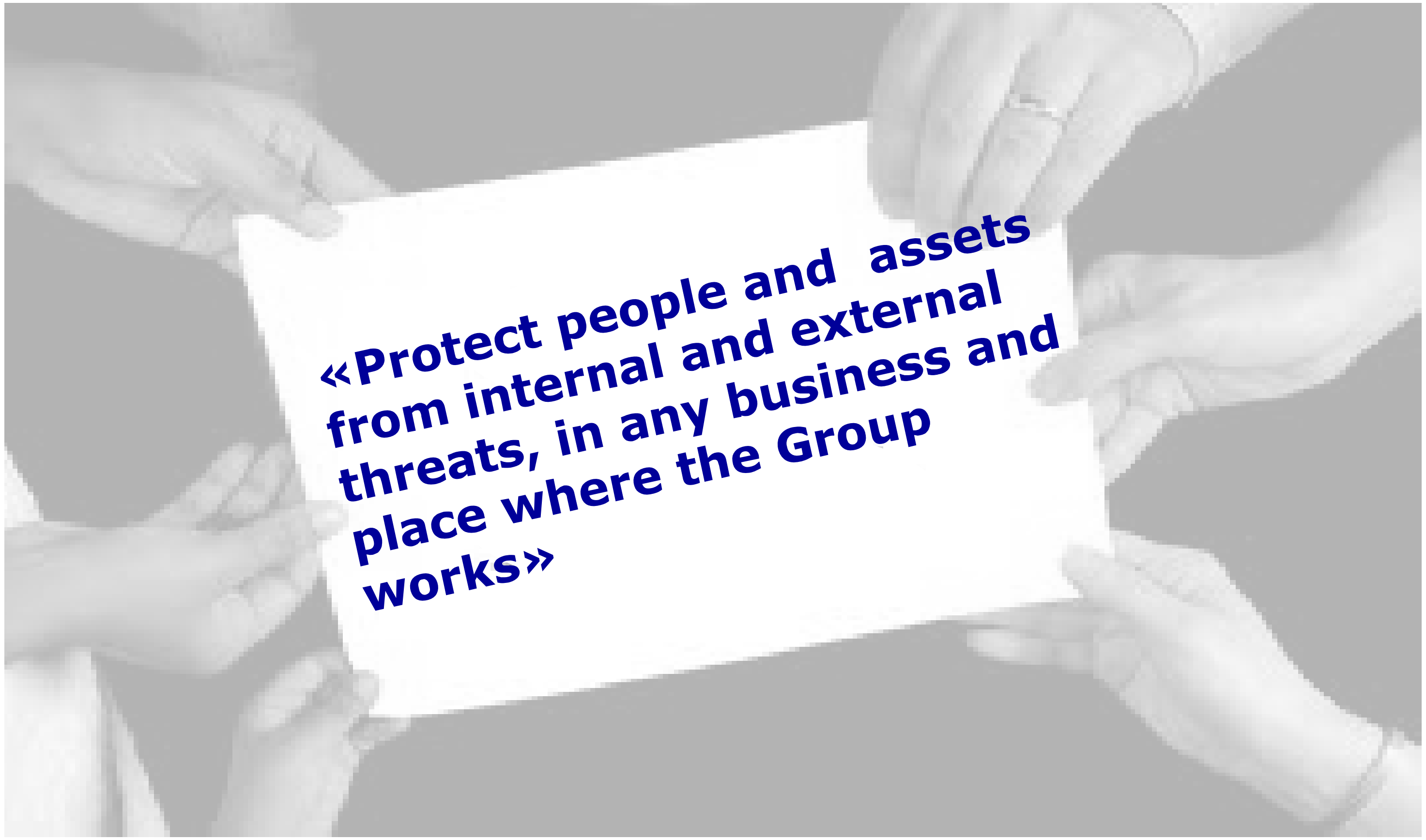
ROMANIA
- Wind energy generation
- Secondo distribution player (35,7%)
- 2,7 mln customers

GRECIA
- Renewable energy production

ITALY
- First energy production player (25% share)
- First distribution player (86%)
- 31 mln customers

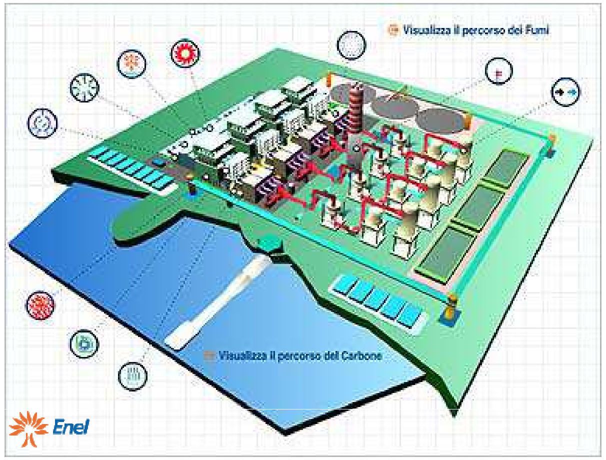
ENERGY IN TUNE WITH YOU.

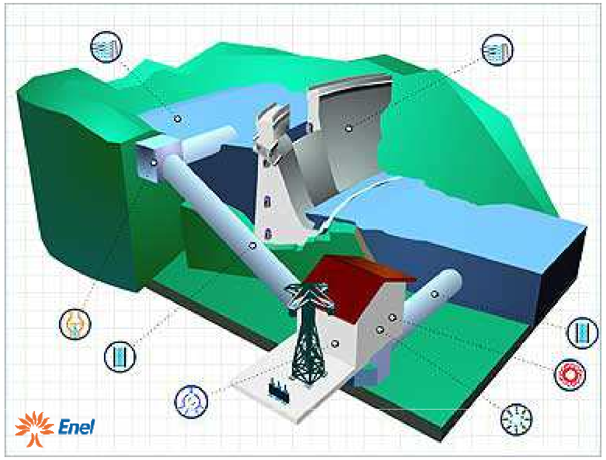
Security Italy

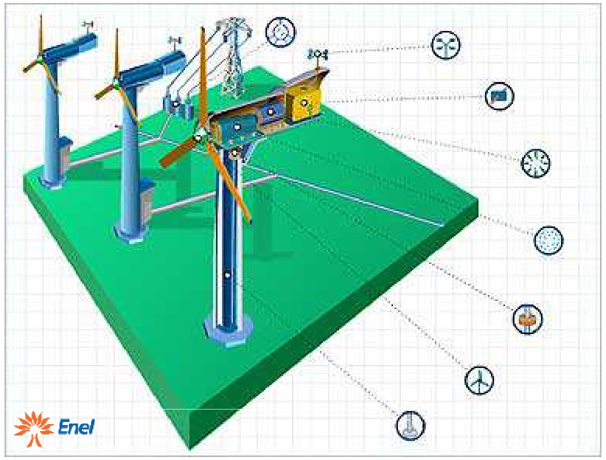


«Protect people and assets from internal and external threats, in any business and place where the Group works»

Enel Italy: generation assets


Visualizza il percorso dei Fumi
Visualizza il percorso del Carbone
Enel





43 thermal power plants

25 installed GW

225 hydroelectric power plants

13 installed GW

398 renewable power plants

More than 3 installed GW

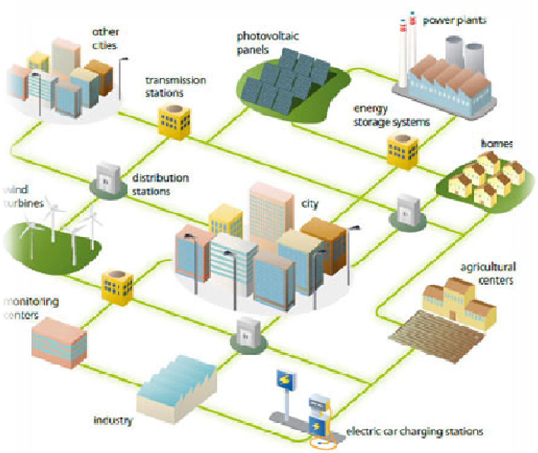
Enel Produzione

Enel Green Power

Enel Italy: distribution assets

More than 1.100.000 km lines

Smart grids



2.000 Primary and
400.000 Secondary Substations

Enel Italy: market assets

L'ENERGIA CHE TI ASCOLTA.

More than 140 Enel Point

Enel Italy: offices

More than 1.200 offices

Enel
L'ENERGIA CHE TI ASCOLTA.

Enel
ENERGY IN TUNE WITH YOU.

Enel Italy: ICT Assets

CED – Data Center

2 data center

L'ENERGIA CHE TI ASCOLTA.

ENERGY IN TUNE WITH YOU.

Infrastructure Security

Role and tasks

- Defines policies, guidelines, standards and technological security systems requirements;
- Defines the analysis method, risk assessment and risk management;
- Process Master Plan of interventions and monitors their implementation by identifying the gaps and proposing corrective actions;
- Ensures compliance with the technological requirements by carrying out the necessary;
- Develop procedures for the management of asset protection systems and participates in the set-up and testing;
- Monitor and assess the overall effectiveness of the security system, identifying the appropriate corrective actions in case of anomalies.

Infrastructure Security

Actions

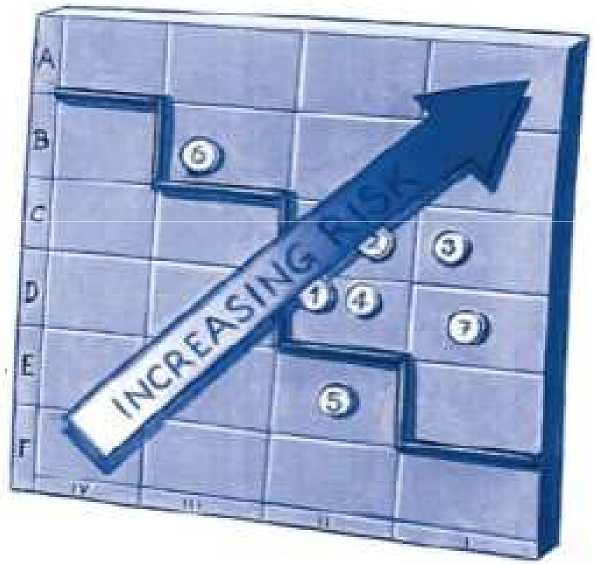
Risk Assessment and Standard	Identify asset categories to be protected, and define - taking into account the risk analysis - countermeasures (systems, processes, procedures) for each type of asset
Infrastructure Security Check	Define and implement a planning in order to check security systems compliance to defined standards
Infrastructure protection improvement	Define security requirements and specifications to adapt systems of security infrastructure (technological systems and procedures)
Masterplan	Planning of the Masterplan for the security infrastructure of the interventions in collaboration with the Divisions / Companies

Infrastructure Security

Risk Assessment

Risk Analysis is a process applied to a specific site with the aim of identifying:

- Critical issues and vulnerabilities of its components,
- Threats to which they are exposed,
- Likelihood that these can occur, damage (impact) to result of an actual or potential attack
- Countermeasures to identified attacks

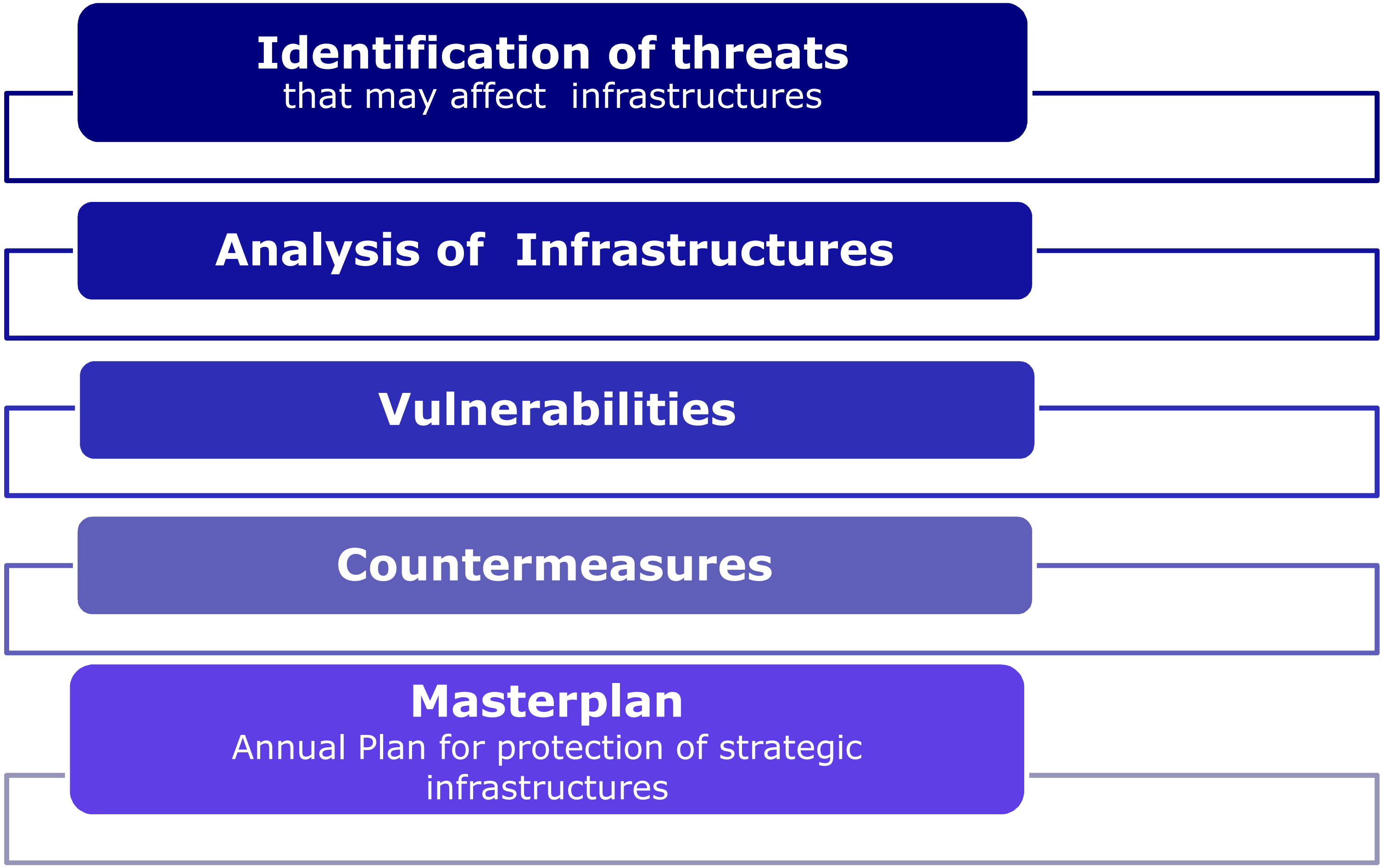


The Risk Analysis is designed to ensure:

- Security of people
- Security of assets
- Continuity of service, safeguarding tangible and intangible assets of the company

Risk Assessment

Threats analysis and vulnerabilities



Identification of threats
that may affect infrastructures

Analysis of Infrastructures

Vulnerabilities

Countermeasures

Masterplan
Annual Plan for protection of strategic infrastructures

Infrastructure Security

Physical Protection Systems

PHYSICAL PROTECTION SYSTEMS (PPS) have three main functions:

1 - Deterring and Detection *(Perimeter protection/technology systems)*

2 - Delay *(Perimeter protection)*

3 - Response *(Security services/Procedures)*

These functions are entering into play every time a malicious act is demonstrated

Infrastructure Security

PPS: Deterring, Detection, Delay and Response

Efficient PPS must **deter malevolent acts** and reduce the possibility that these develop into security incidents.

Deterring: Convince potential intruders that an intrusion attempt will have low probability of success.

Detection: perimeter protection and electronic surveillance systems reduce the probability that an intrusion attempt turns into a successful attack.

Delay: Physical barriers may be used to delay intruders from reaching critical elements of energy installations. They aim at reducing the vulnerability in cases that the first layers of protection have failed.

Response: Security services (guards) and police forces are entitled to respond in case of intrusion in order to mitigate risks.

Infrastructure Security

Example

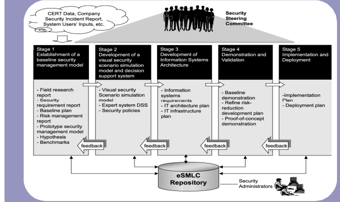
Perimeter Protection

- Fences
- Walls
- Door locks
- Restricted entrance

Technology System

- Electronic surveillance systems (TVCC/Sensors)
- Access control system
- Anti-intrusion system

Security services


CERT Data, Company Security Incident Report, System Users' Inputs, etc.
Security Steering Committee
Stage 1 Establishment of a baseline security management model
Stage 2 Development of a visual security scenario simulation model and decision support system
Stage 3 Development of Information Systems Architecture
Stage 4 Demonstration and Validation
Stage 5 Implementation and Deployment
- Field research report
- Security requirement report
- Baseline plan
- Risk management report
- Prototype security management model
- Hypothesis
- Benchmarks
- Visual security Scenario simulation model
- Expert system DSS
- Security policies
- Information systems requirements
- IT architecture plan
- IT infrastructure plan
- Baseline demonstration
- Refine risk-reduction development plan
- Proof-of-concept demonstration
-Implementation Plan
- Deployment plan
feedback
feedback
feedback
feedback
eSMLC Repository
Security Administrators

Procedures

Infrastructure Security

Concentric protective barrier standard

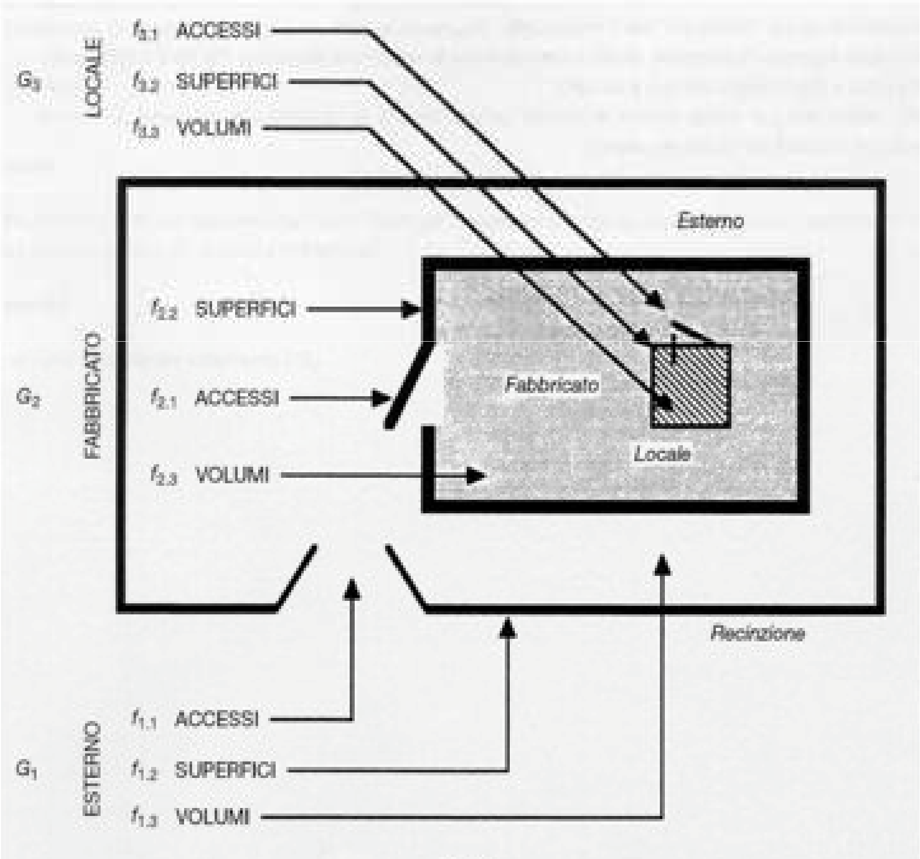


Fig. 4

Given the conformation and characteristics of a site to be protected, are normally identified three concentric areas of protection:

1. **Area outside place to protect (G1), includes perimeter fencing, access gates and not built internal areas close to the fence;**

2. **Intermediate area of protection (G2), includes buildings, equipment rooms, all internal sensitive areas**

3. **Protection of particular local sensitive internal perimeter G3**

Risk Assessment
Risk Matrix

LIKELIHOOD

	Minor Negligible economical-social damage	*Moderate* Moderate economical-social damage	*Significant* Significant economical-social damage	*Extreme* Fatalities Huge economical-social damage
Frequent Occurs frequently	Low	Medium	High	High
Probable It is known to occur / occured before	Low	Medium	High	High
Occasional Could occur	Low	Medium	Medium	Medium
Remote Not likely to occur	Low	Low	Low	Low

IMPACT

Risk Level

Focus on: Assets Vs Threats

	Power Plants	Lines	Substations	Civil Sites	Enel Stores
Theft	High	High	High	Low	Low
Demonstration	High	Low	Low	Medium	Low
Protest	High	Low	Low	Medium	Low
Attack	Medium	Low	Low	Low	Low
Aggression	Medium	Low	Low	Medium	High
Terrorism	Medium	Medium	Low	Low	Low

Risk Level

Focus on: Assets and Countermeasures

	Power Plants	Lines	Substations	Civil Sites	Enel Stores
Technology System	✓	✓	✓	✓	✓
Perimetral Protection	✓	✗	✓	✓	✗
Security Guard	✓	✗	✗	✓	✓
Procedures	✓	✓	✓	✓	✓

Infrastructure Security

Security Control Room

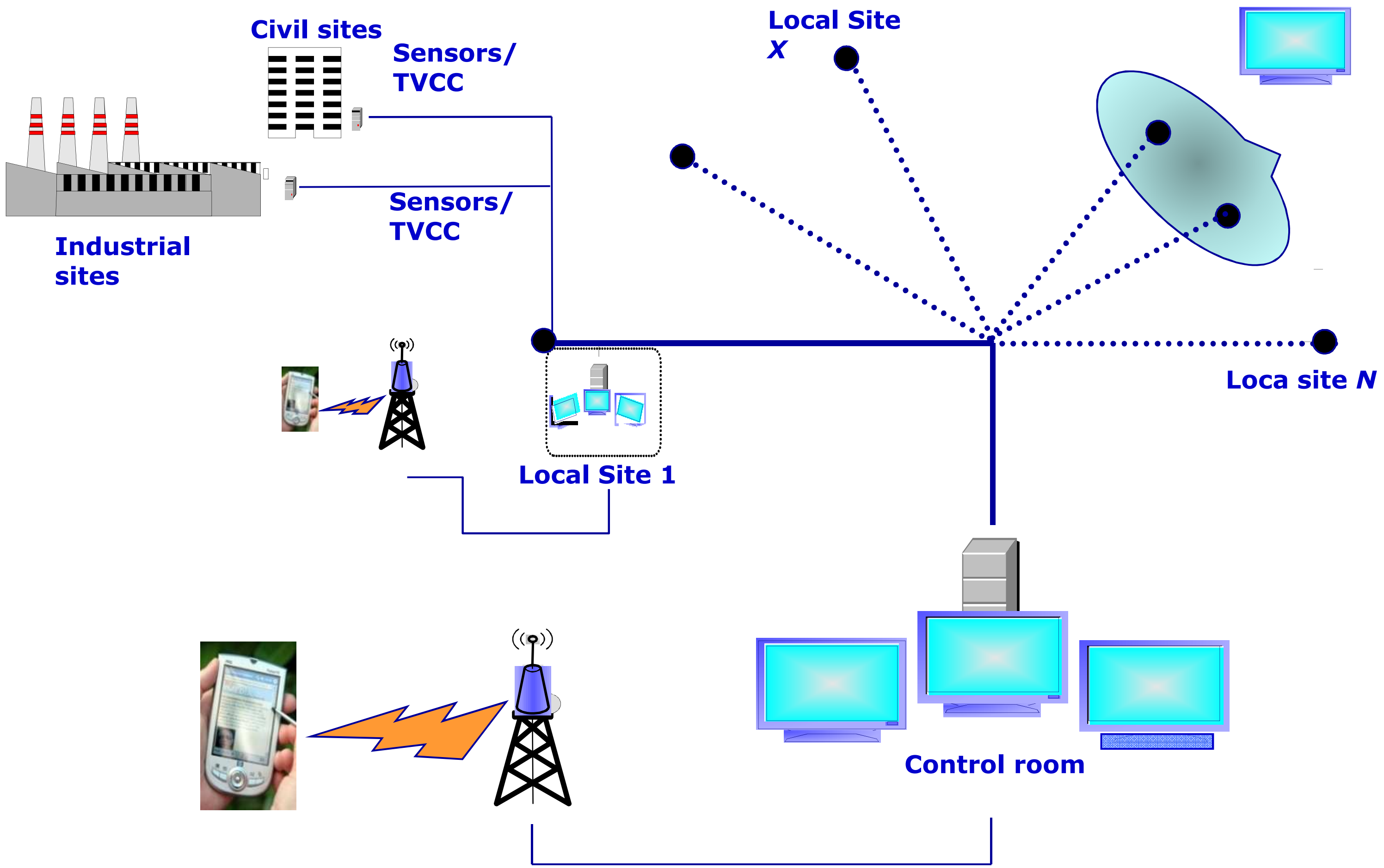
Management of warnings coming from physical protection systems

Security event reaction capability enhancement

Integrations of warnings and alarms from infrastructure security systems

Infrastructure Security

Security Control Room



Infrastructure Security

Enel’s technologies / 1

Thermal camera coupled
with a PTZ camera

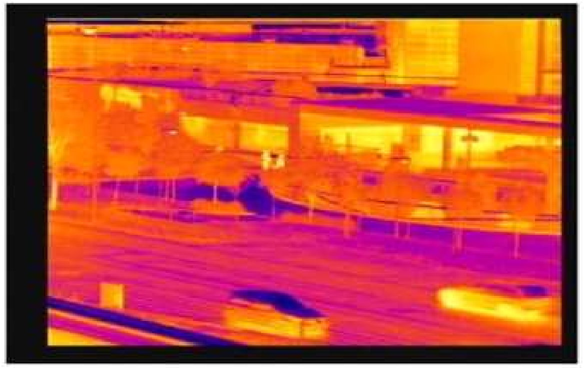
Motion dectector

IR barrier

Infrastructure Security

Enel's technologies / 2

Piezometric Detector



Thermal Cameras

Security Standards - CEI 79

Defining rules for anti-intrusion devices

- **CEI 79 Anti-intrusion systems, burglar alarm and duress - (Particular requirements for equipment / Particular requirements for installations burglary and anti-intrusion);**

- **CEI 79- 2 Anti-intrusion systems, burglar alarm and duress (Particular requirements for equipment);**

- **CEI 79- 3 Anti-intrusion systems, robbery and anti-aggression (Particular requirements for installations burglary and anti-intrusion);**

- **CEI 79- 4 Anti-intrusion systems, burglar alarm and duress (Particular requirements for access control);**

Security Standards - CEI 79 (EN 50131-3)

Defining rules for anti-intrusion devices

- **CEI 79- 5 Communications protocol for the transfer of security alarms - Part 1: the transport layer;**

- **CEI 79- 6 Communications protocol for the transfer of security alarms - Part 2: Application Layer;**

- **CEI 79- 11 Centralization of security alarms. System Requirements;**

- **EN 50133-1 (CEI 79 - 14) Alarm systems - Access control systems for use in security applications. Requirements of the systems;**

- **EN 50131-1 (CEI 79- 15) Alarm systems - Intrusion Alarm Systems - General requirements.**

Security Control Room

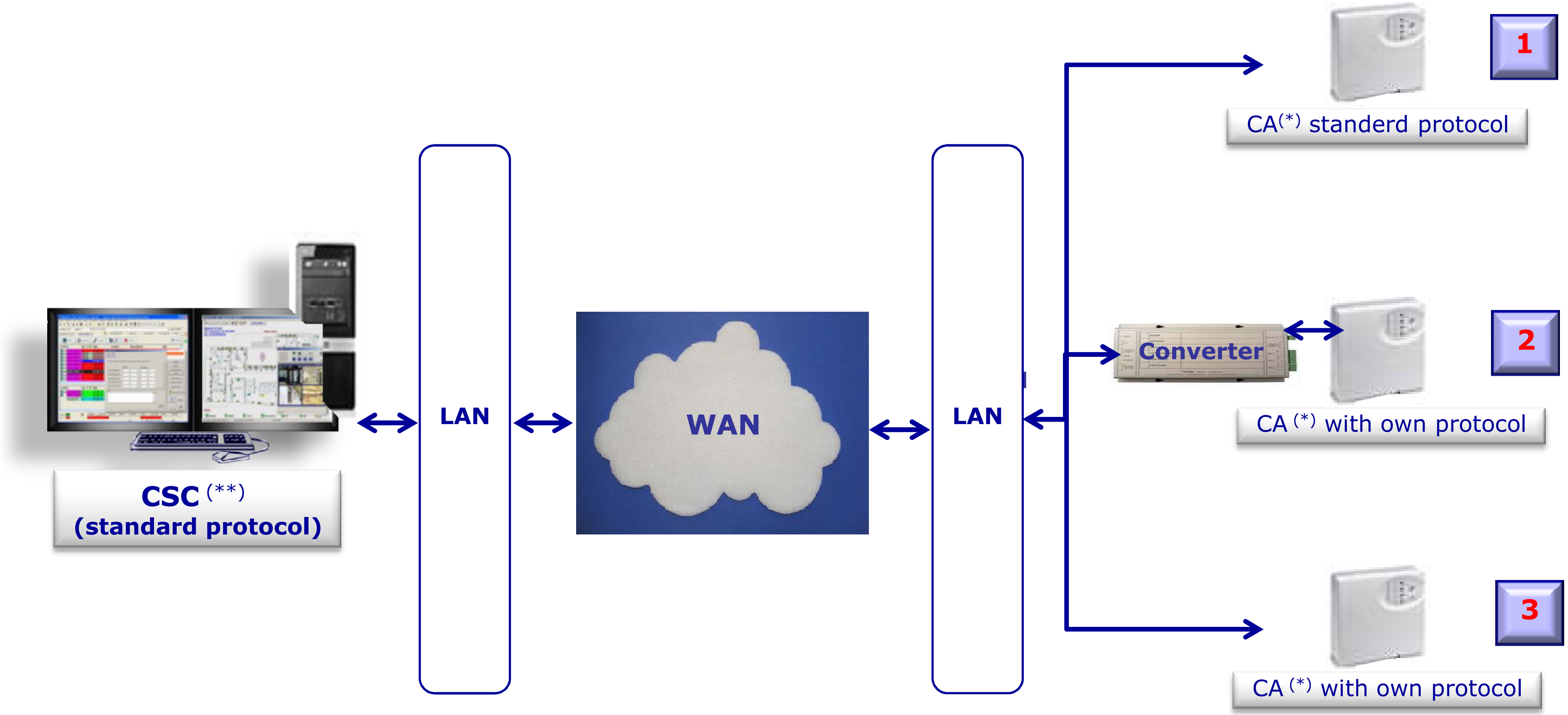
Standard Communication Protocol (CEI 79-5/6)

A communication protocol is a set of rules defined in order to facilitate communication between two or more devices.

It's clear the importance of a standard communication protocol with the involvement of appropriate national and international bodies.

Security Control Room

Standard Communication Protocol (CEI 79-5/6/11)



(*) Centralized counter intrusion system
(**) Monitoring and Control Center

Security Control Room

Standard Communication Protocol (CEI 79-5/6)

❑ Provides **bi-directional exchange of information** between the *Centralized Counter Intrusion System* and the *Monitoring and Control Center*, through the following classes of performance: information security and reliability of the system, time required to report the information to the *Monitoring and Control Center,* detail level of exchanged information

❑ Defines the **rules for exchanging information** through the general structure of the data packets exchanged, structure of alarms packages and sensors

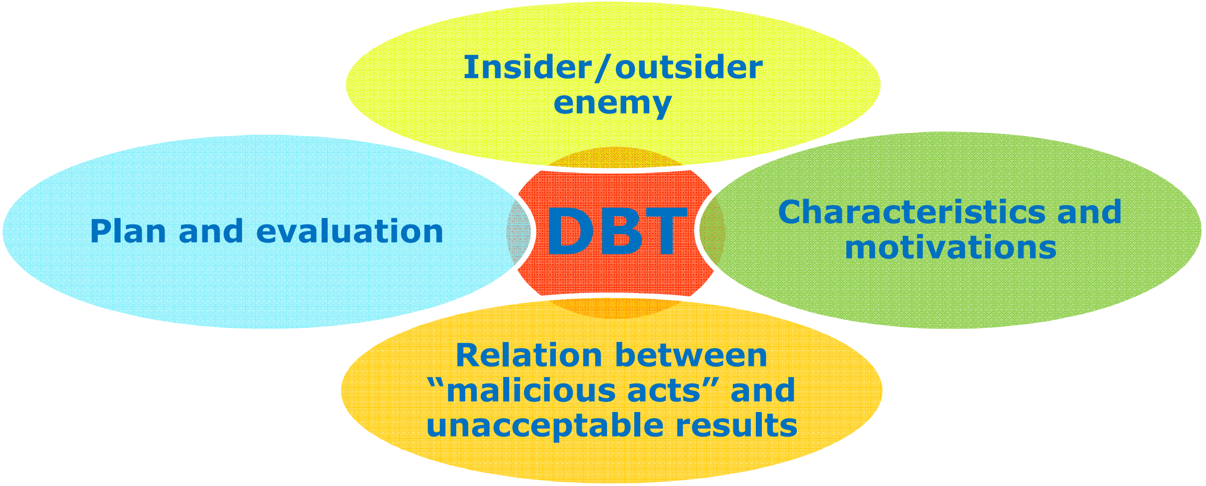
Design Basis Threat (DBT)

Definition

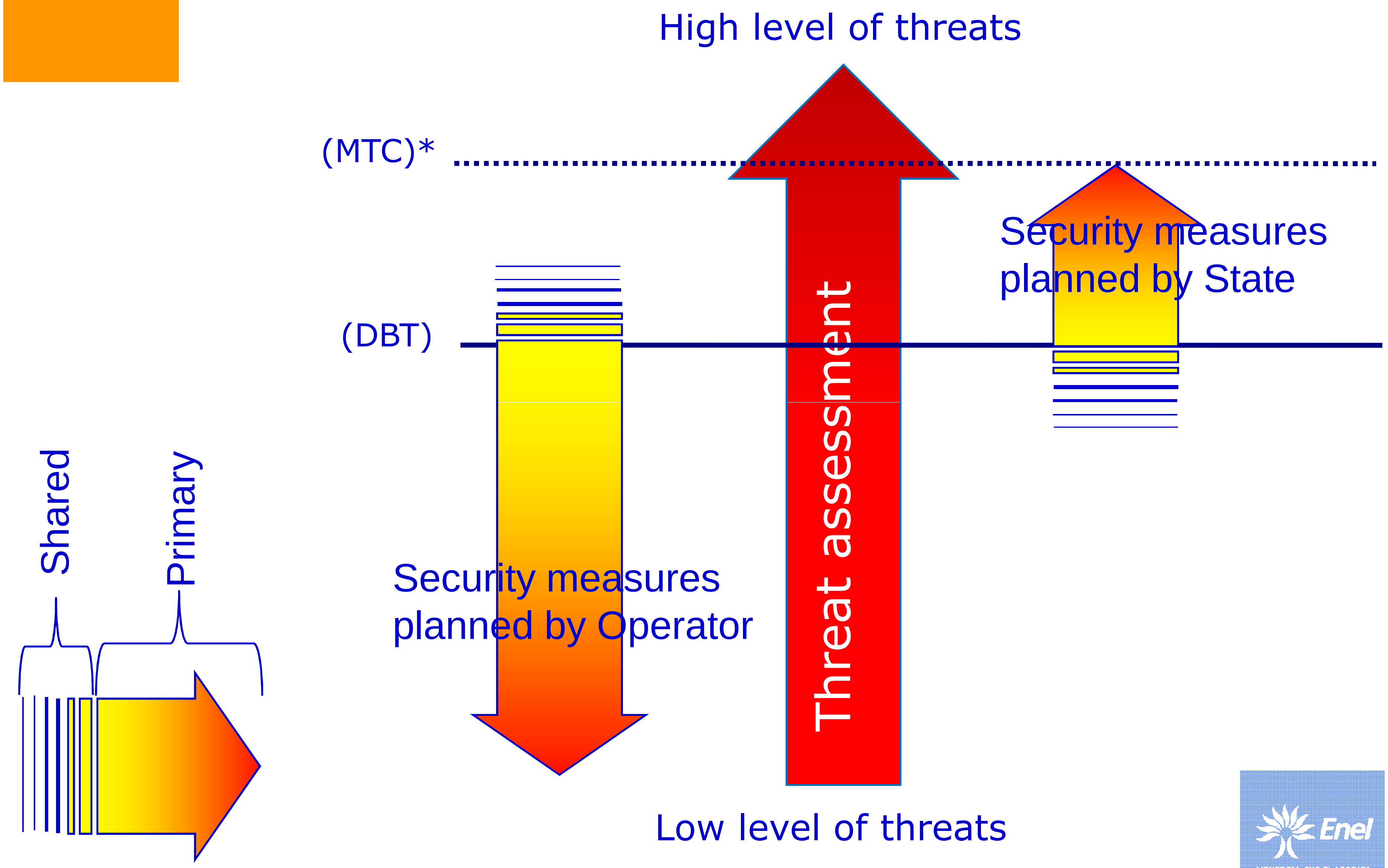
WHAT IS A "DESIGN BASIS THREAT" (DBT)

- Document that describes motivations, intentions and capabilities of potential enemy (insider/outsider) against whom plan and evaluate protection systems

- Document is provided by reliable information and other data relating to threats (planned or possible)


Insider/outsider enemy
Plan and evaluation
DBT
Characteristics and motivations
Relation between "malicious acts" and unacceptable results

Design Basis Threat (DBT)



* Maximum Threat Capacity