



# Processes, structures and organization for infrastructure protection in Italy

Ing. Gaetano Condorelli  
Head of Infrastructure Security and Crisis Management

*September 12nd and 13th, 2013  
Brussels, Centre A. Borschette*

*Testing Security: the Critical Infrastructure Operator's View*

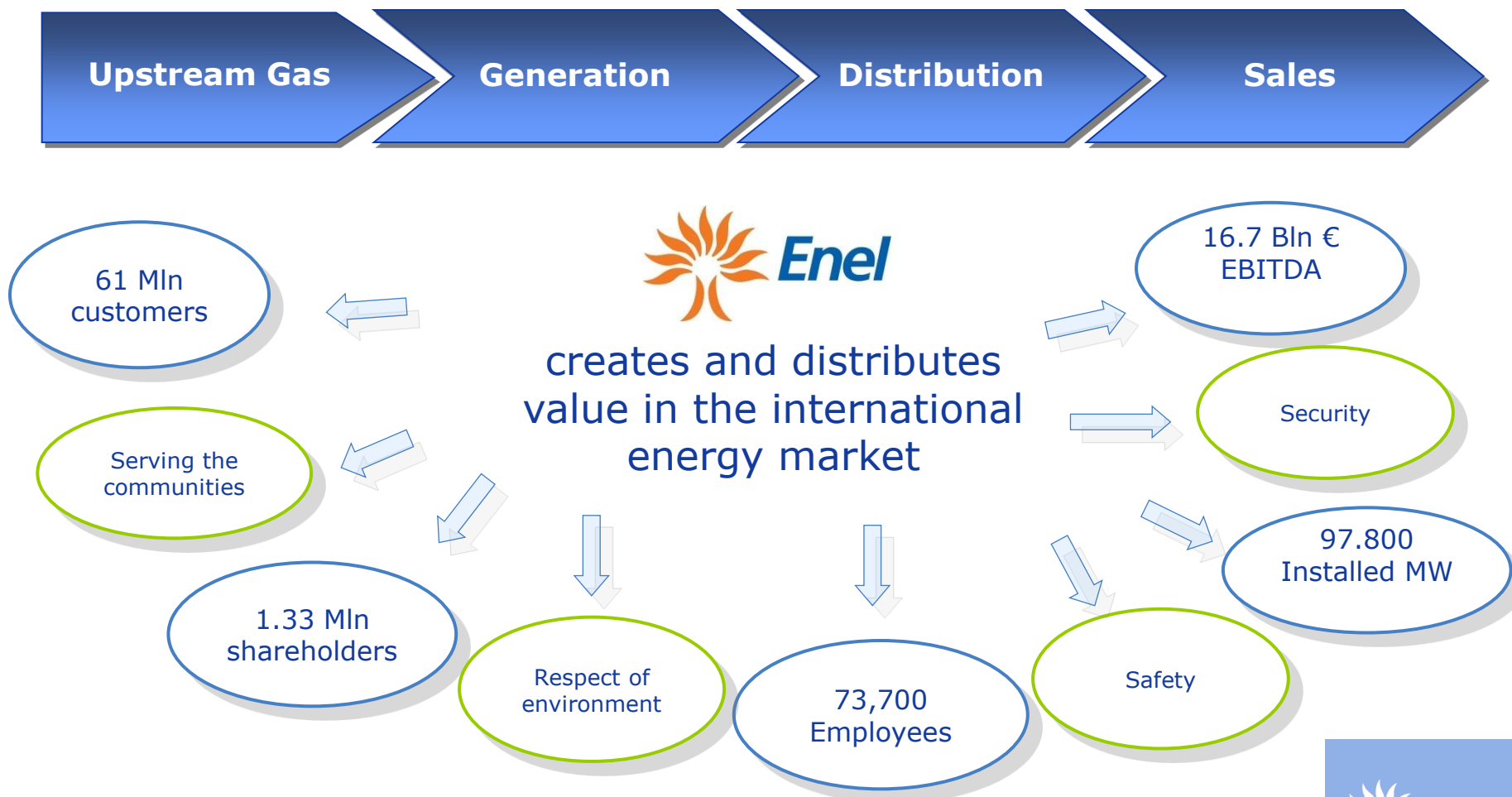
***ERNCIP Workshop***

# Index

- ☐ **Enel Overview**
- ☐ **Security Italy**
- ☐ **Risk Assessment**
- ☐ **Infrastructure Security**
- ☐ **Crisis Management**

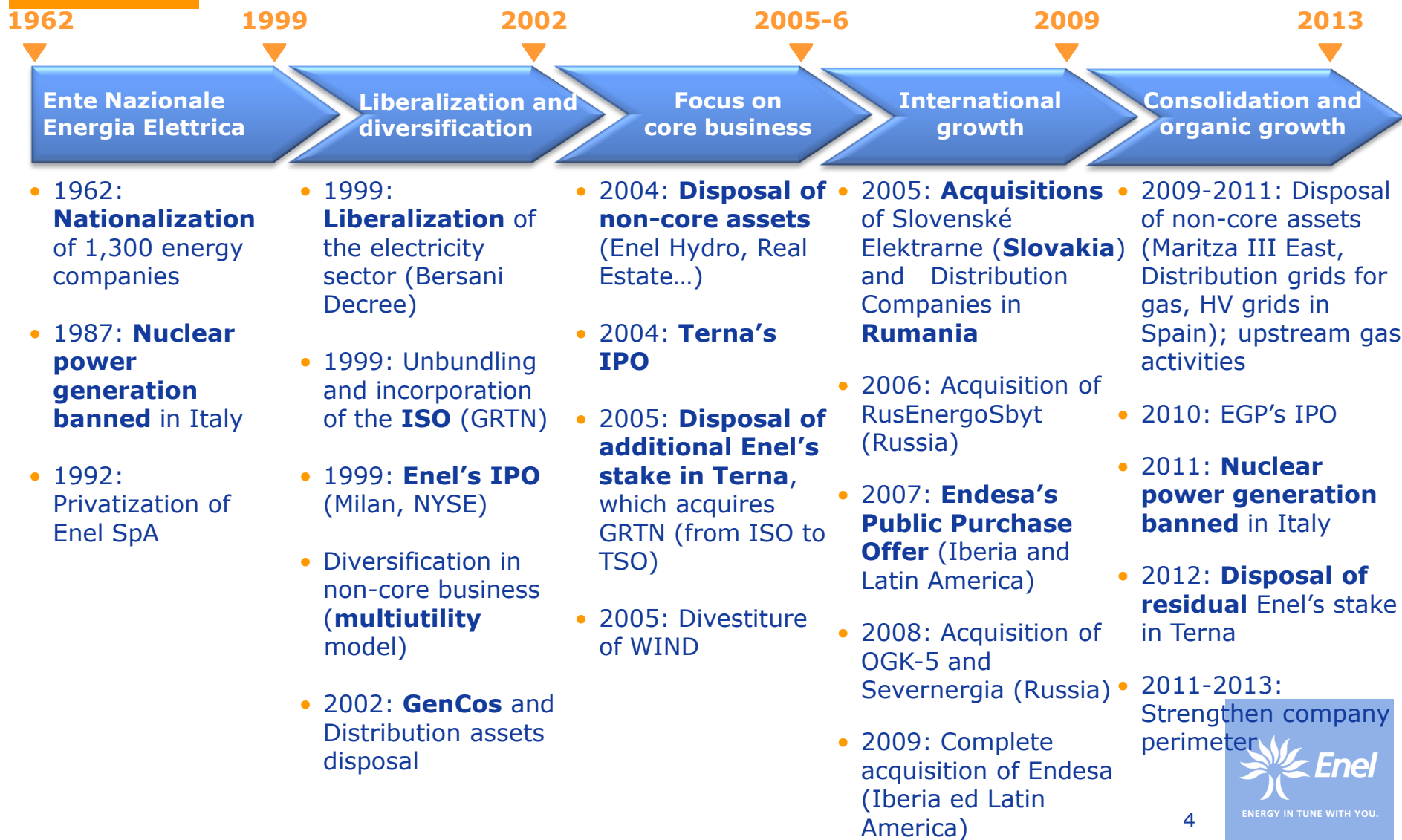
# Enel overview

## Integrated energy player



# Enel overview

## Enel's transformation milestones

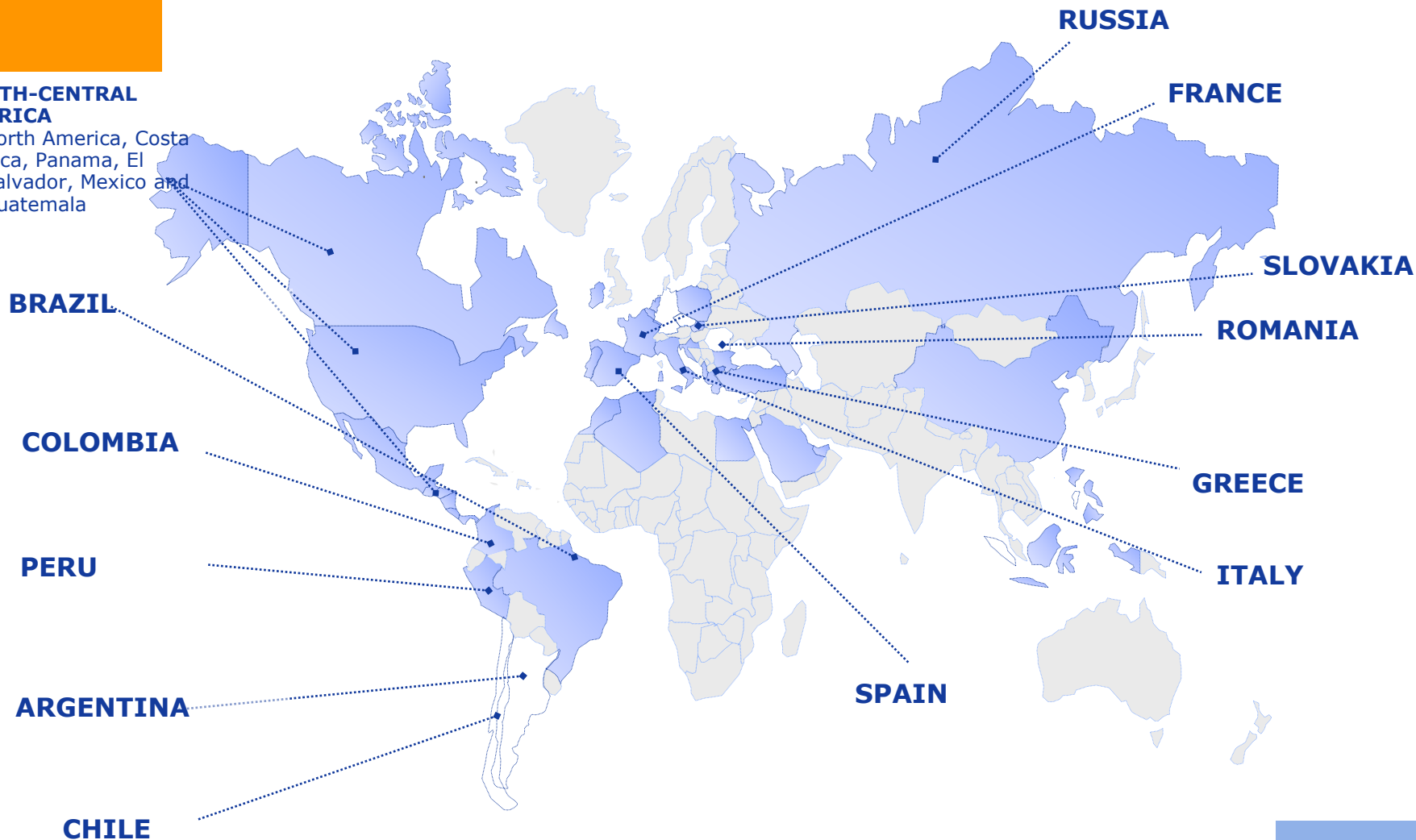


# Enel overview

## Focus on major areas of presence

### NORTH-CENTRAL AMERICA

- North America, Costa Rica, Panama, El Salvador, Mexico and Guatemala



# Index

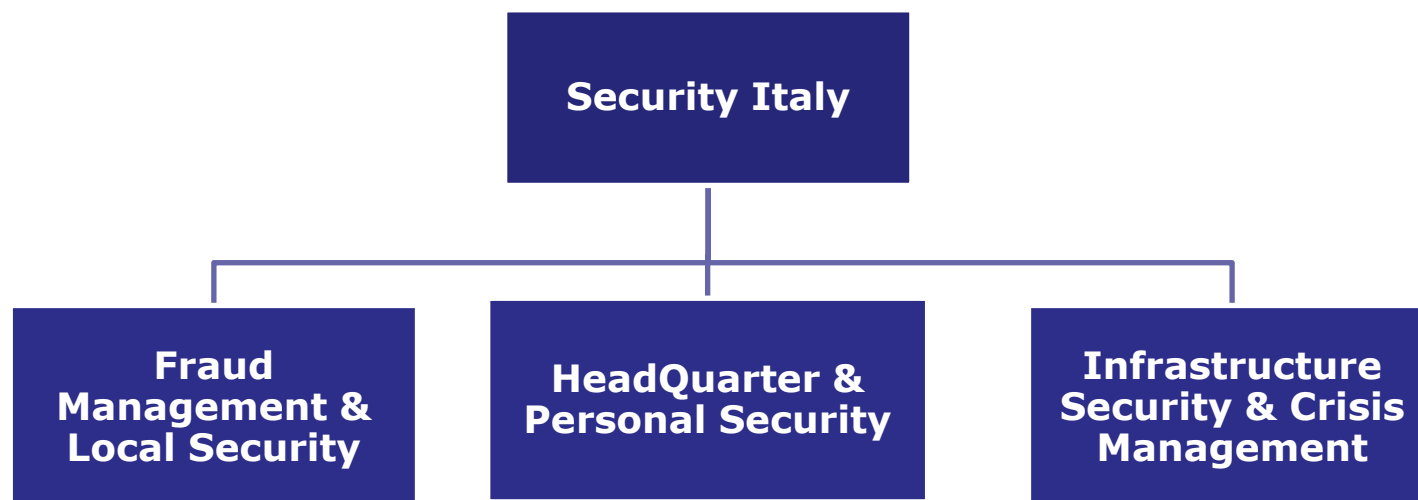
- ☐ Enel Overview
- ☒ **Security Italy**
- ☐ Risk Assessment
- ☐ Infrastructure Security
- ☐ Crisis Management

# Security Italy



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

# Security Italy





## **Enel Italy: generation assets**



**43 thermal power plants: 25 installed GW**



**225 hydroelectric power plants: 13 installed GW**



**398 renewable power plants: more than 3 installed GW**

## **Enel Italy: distribution assets**



**More than 1.100.000 km lines**



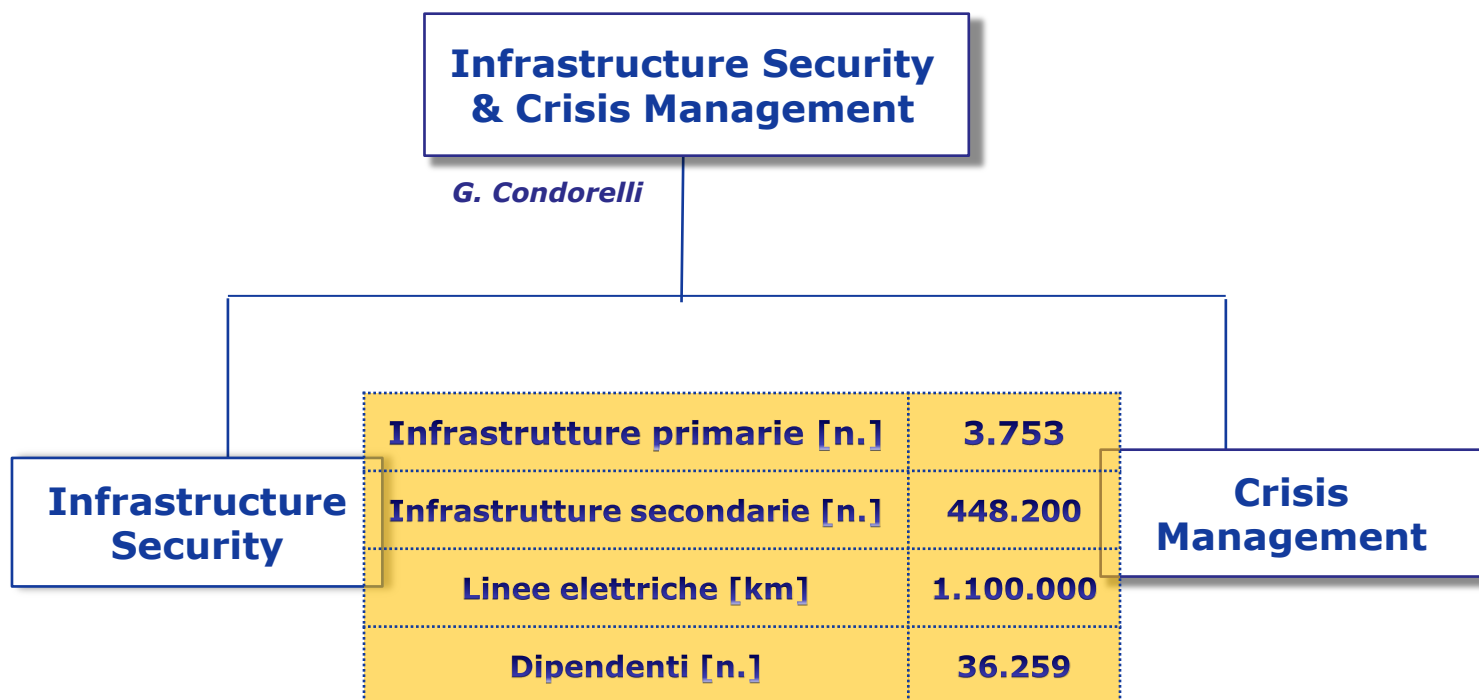
**2.000 Primary and 400.000 Secondary Substations**



**31 million customers**

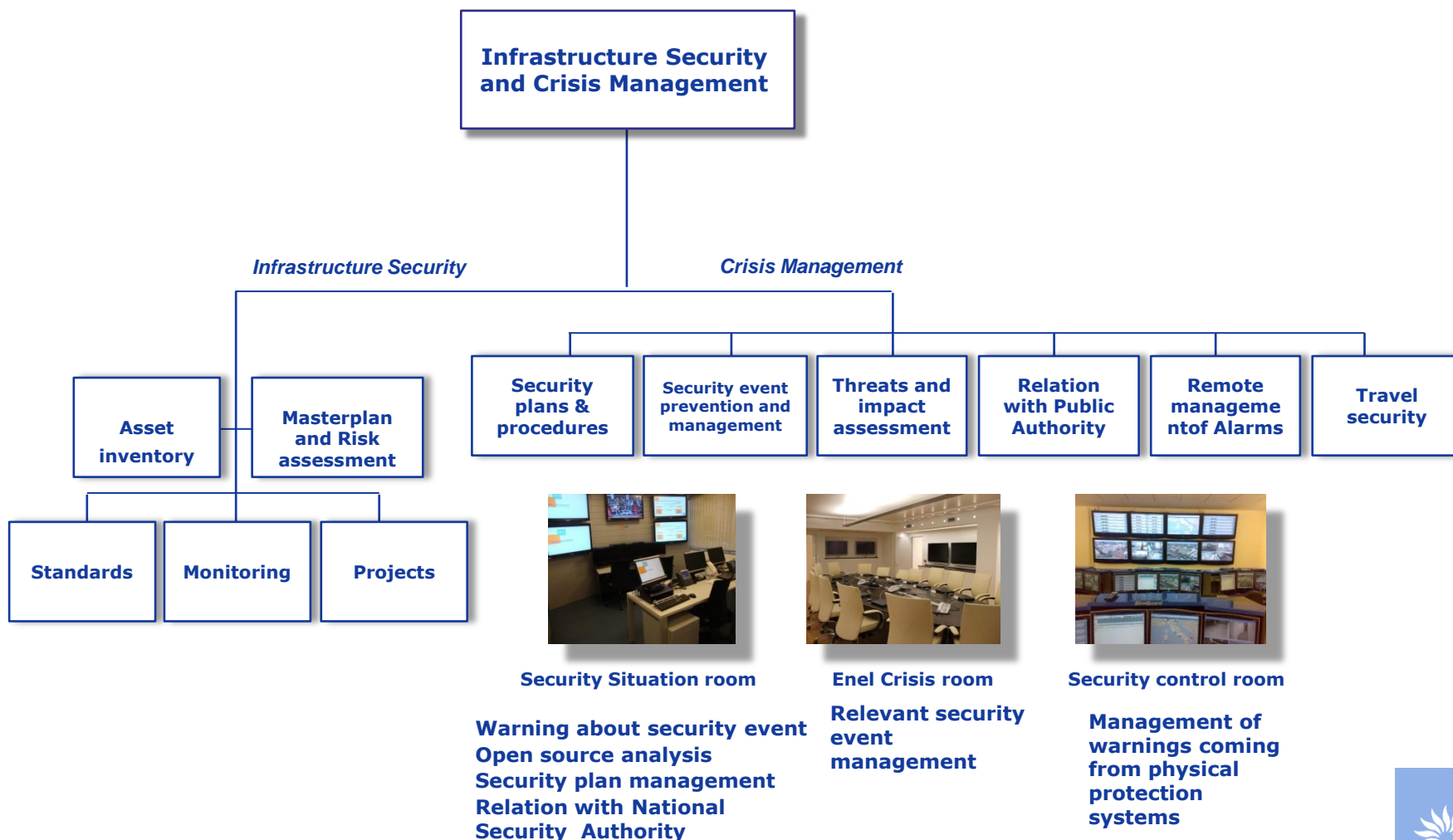
# Security Italy

## Infrastructure Security and Crisis Management



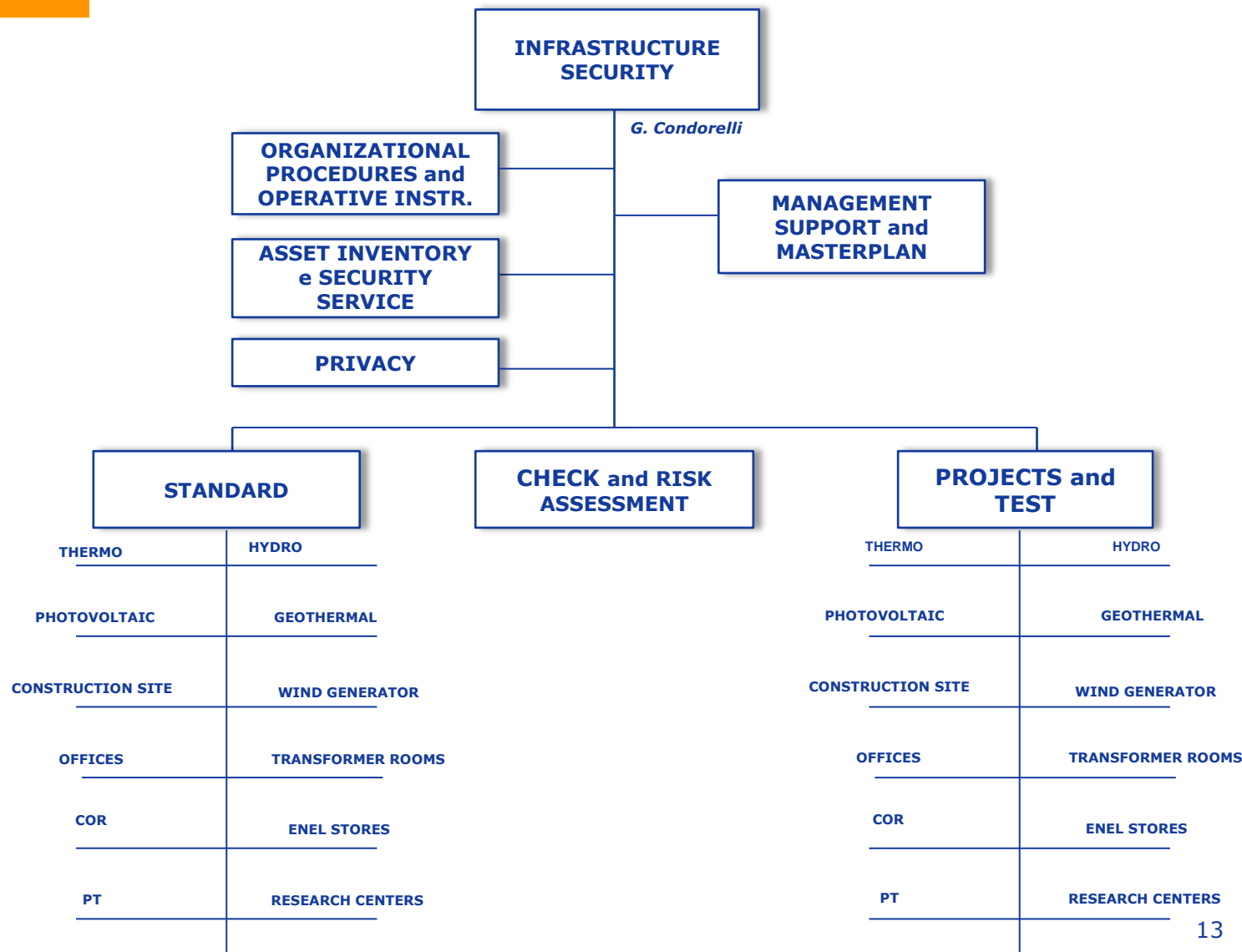
# Security Italy

## Focus on Infrastructure Security and Crisis Management



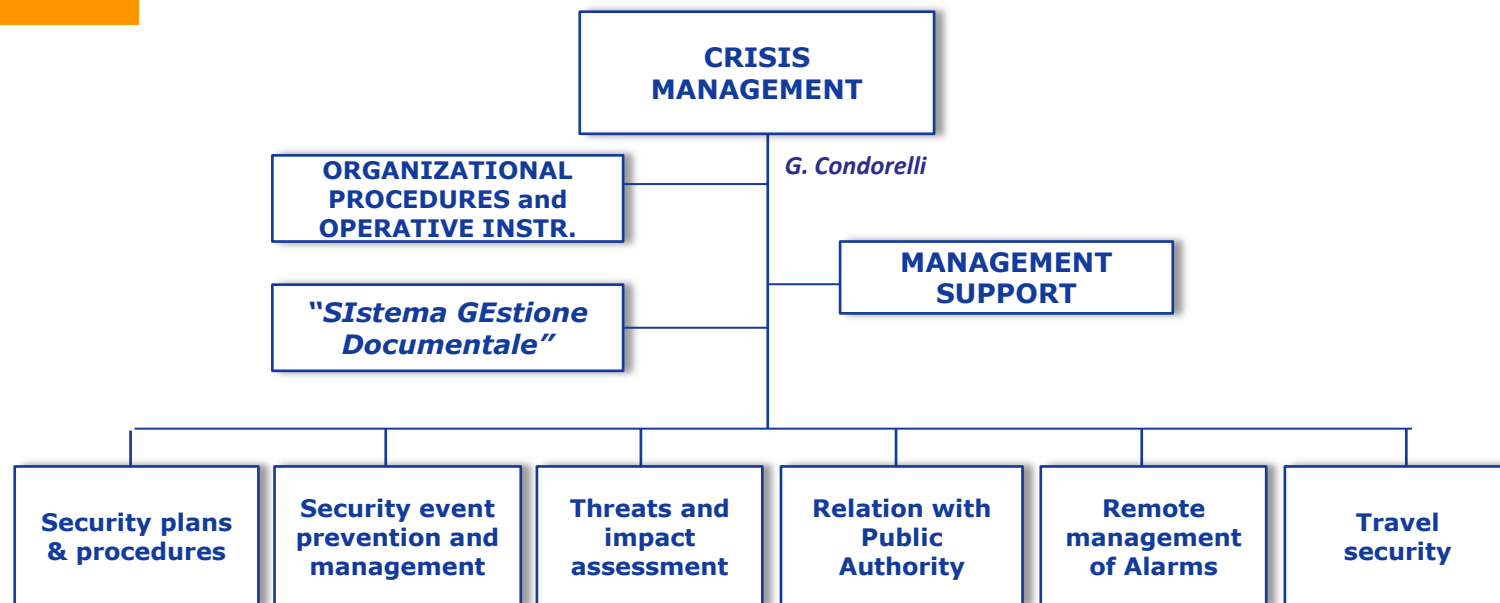
# Infrastructure Security and Crisis Management

## Focus on Infrastructure Security



# Infrastructure Security and Crisis Management

## Focus on Crisis Management



**Security Situation room**

Warning about security event  
Open source analysis  
Security plan management  
Relation with National Security Authority



**Enel Crisis room**

Relevant security event management



**Security control room**

Management of warnings coming from physical protection systems

# Index

- ❑ Enel Overview
- ❑ Security Italy
- ❑ **Risk Assessment**
- ❑ Infrastructure Security
- ❑ Crisis Management

# Risk Assessment

## Risk Assessment Process

Risk Assessment is a process applied to a specific perimeter of intervention in order to identify:

**vulnerabilities** of the infrastructures

**threats** to which they are exposed and the **probability** that these can happen

**impact** and damages deriving from a threat

**countermeasures** for prevention

Risk Assessment is addressed to contribute to service continuity and safeguard of business material and immaterial assets



# Risk Assessment

## Business Impact Analysis



### Business Impact Analysis

- **Scenario description, identification of the scope of intervention**
- **Identification of strategic infrastructures and their interdependencies**
- **Assessment of direct and indirect impacts resulting from their partial or total unavailability**

# Risk Assessment

Threats analysis and vulnerabilities

**Identification of  
threats**

that may affect  
infrastructures

**Analysis of  
vulnerabilities**

of infrastructures

**Risk Analysis**

**Masterplan**

Annual Plan for  
protection of strategic  
infrastructures

# Risk Assessment

## Risk Matrix

### PROBABILITY

*Frequent*

Occurs frequently

*Probable*

It is known to occur /  
occured before

*Occasional*

Could occur

*Remote*

Not likely to occur



Low	Medium	High	High
Low	Medium	Medium	High
Low	Low	Medium	Medium
Low	Low	Low	Low

*Minor*

Negligible  
economical-social  
damage

*Moderate*

Moderate  
economical-social  
damage

*Significant*

Significant  
economical-social  
damage

*Extreme*

Fatalities  
Huge economical-  
social damage

### SEVERITY

# Index

- ❑ Enel Overview
- ❑ Security Italy
- ❑ Risk Assessment
- ❑ **Infrastructure Security**
- ❑ Crisis Management

# Infrastructure Security

## Protection systems

### Passive Security

- *fences*
- *fixtures*
- *storehouses*
- *sensitive locals*
- *gates*



### Threat Analysis

- *thefts*
- *intrusions*
- *sabotage*
- ...



### Vulnerability Analysis

- *by type of site*
- *specific site*
- *specific context*

### Active Security

- *video surveillance*
- *monitoring*
- *access control*
- *anti intrusion*
- *procedures*



# Infrastructure Security

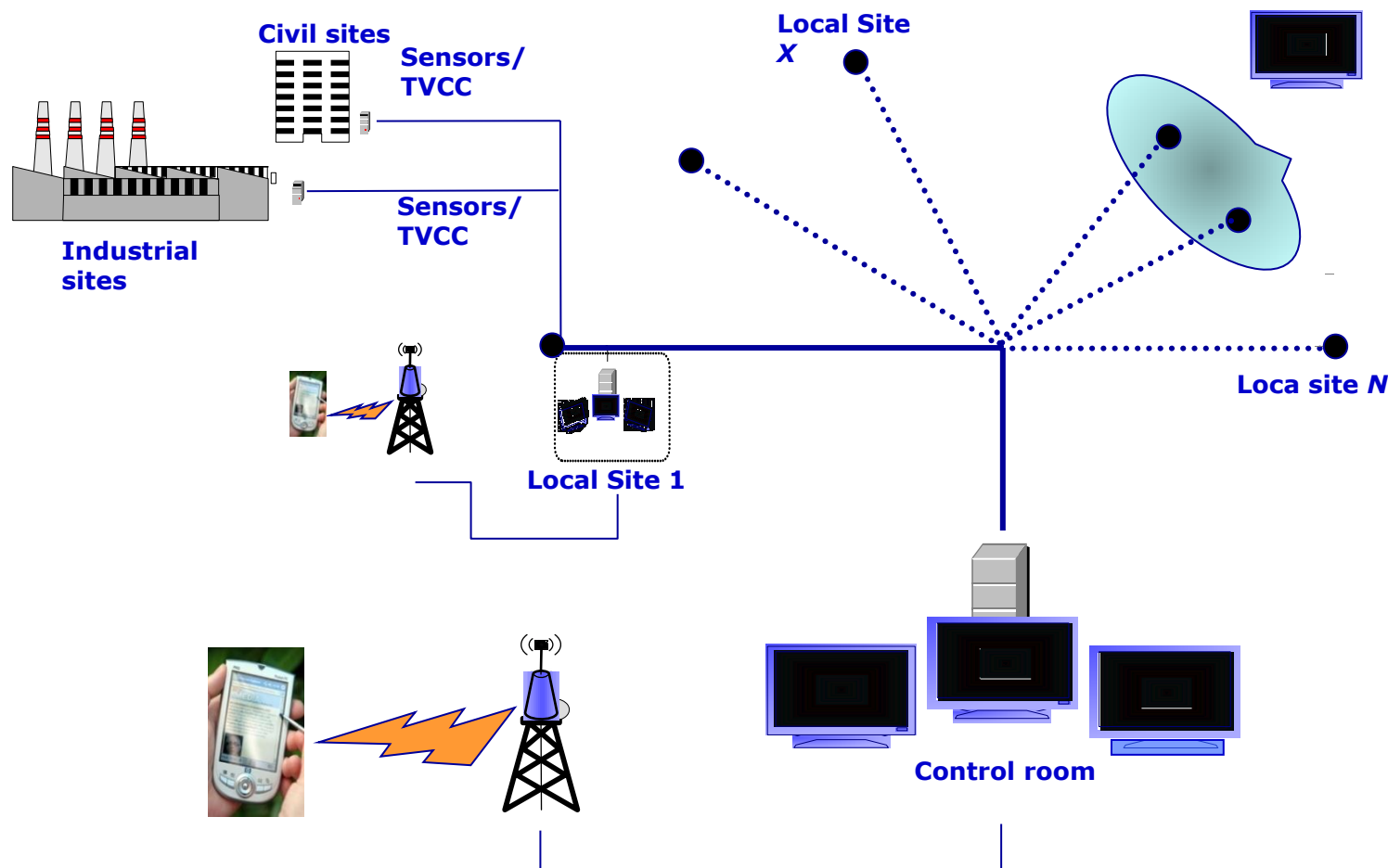
## Security Control Room

- ❑ **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



# Security Control Room

## Standard Communication Protocol

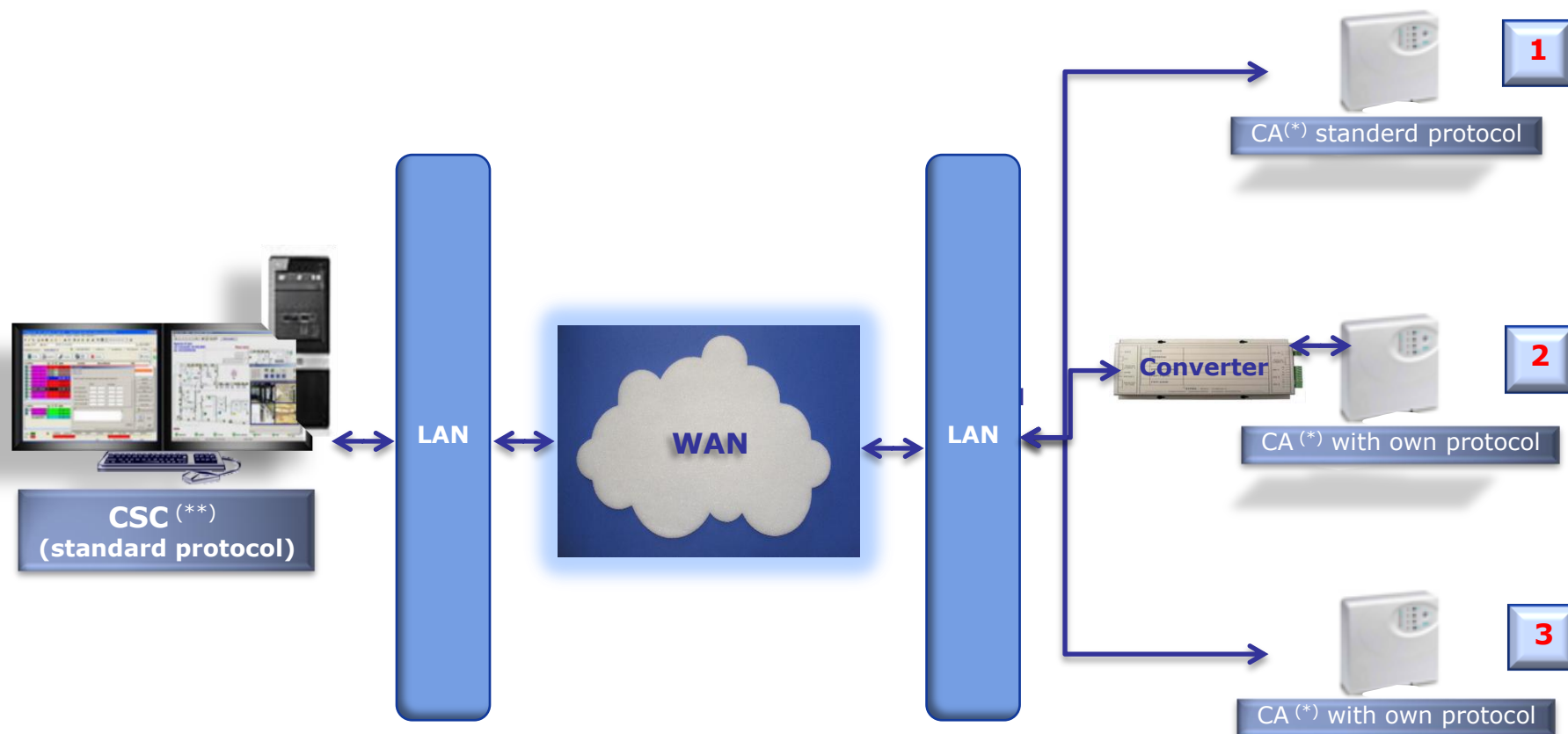
A **communication protocol** is a set of rules defined in order to facilitate communication between two or more devices.

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



(\*) Centralized counter intrusion system

(\*\*) Monitoring and Control Center

# Security Control Room

## Standard Communication Protocol

- ❑ 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

# Index

- ❑ **Enel Overview**
- ❑ **Security Italy**
- ❑ **Risk Assessment**
- ❑ **Infrastructure Security**
- ❑ **Crisis Management**

# Crisis Management in Enel



- Development of Crisis Management System
- Test through periodic simulations
- Development of emergency procedures

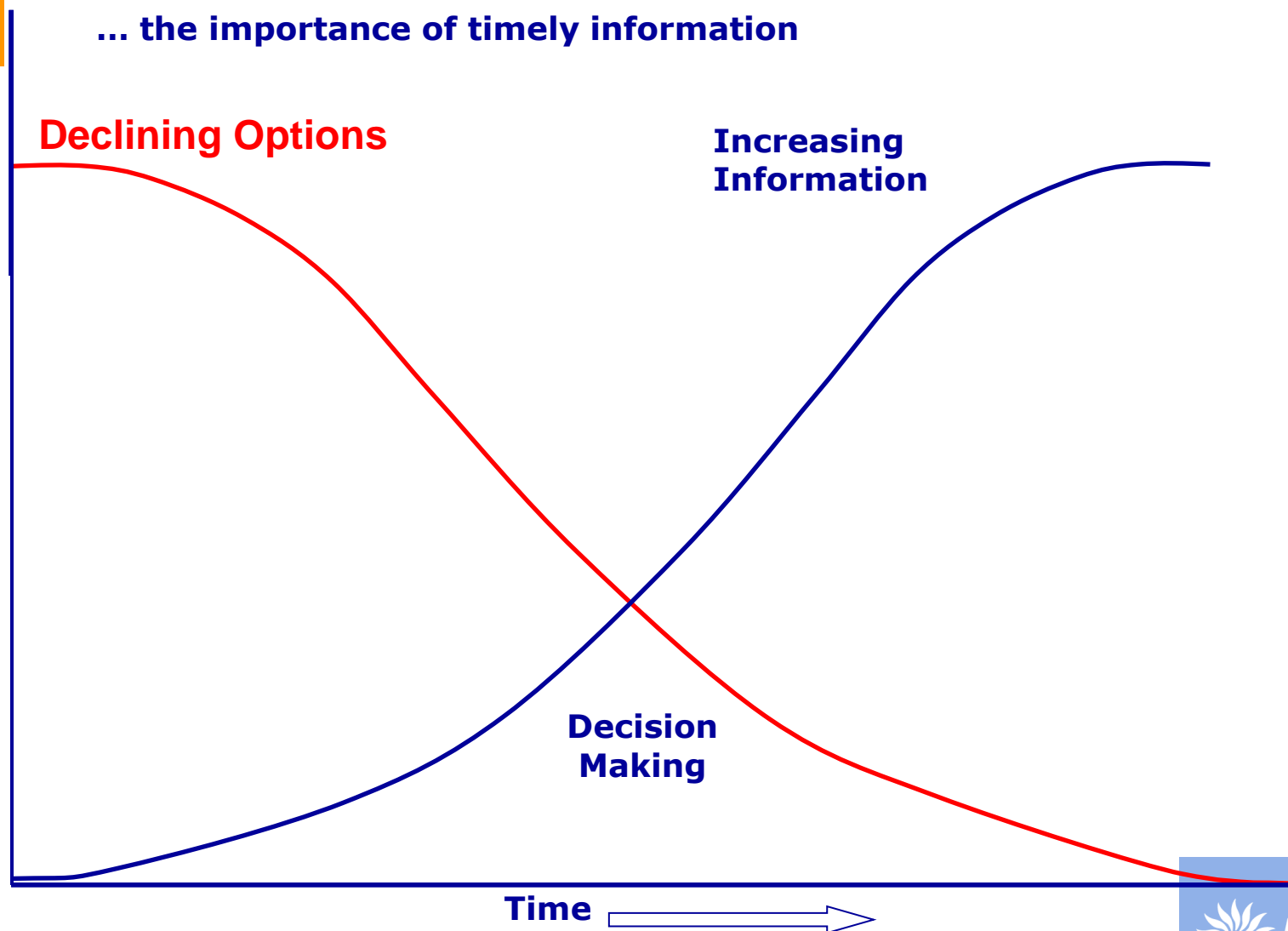
- Coordination with Civil Protection, Ministry of Interior, Ministry of Foreign Affairs
- Coordination with other infrastructures operators (e.g. TSO)



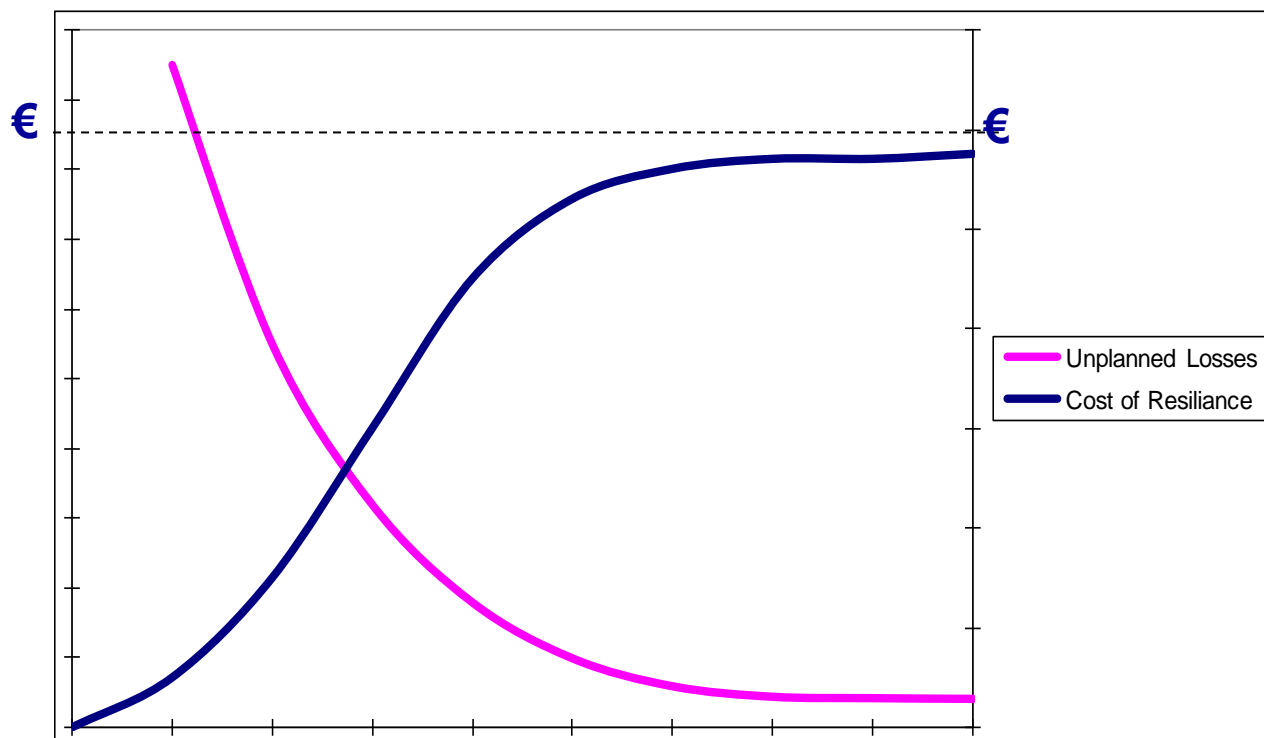
- Development, operation and maintenance of crisis and emergency facilities (e.g. crisis room)

## Decision making during a crisis...

... the importance of timely information

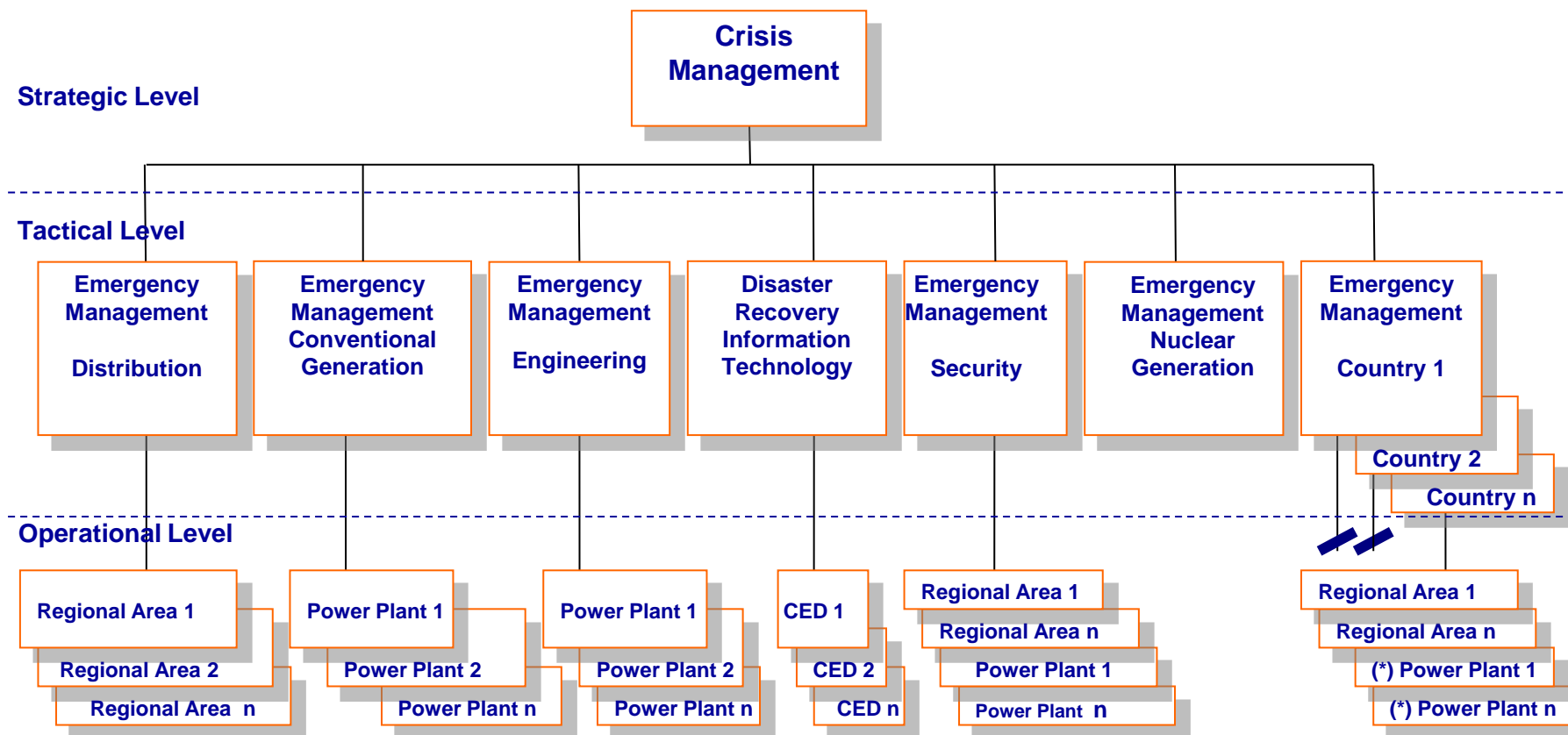


## Cost of Resilience



**If unplanned losses are apparently well-contained, it is tempting to economise by cutting back on Resilience ... but small investments in Resilience may produce very high Unplanned Losses**

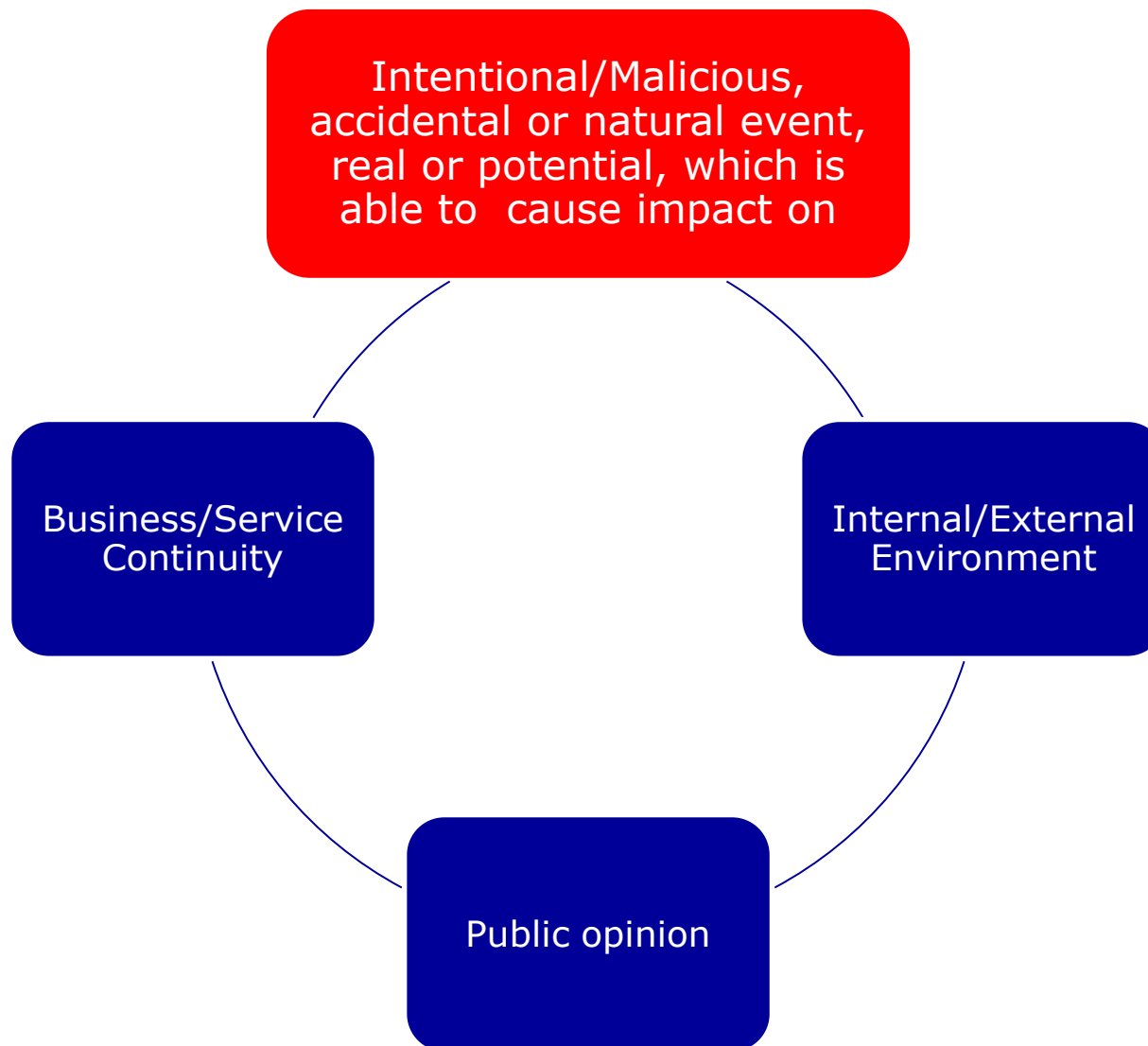
# Crisis Management in Enel



(\*) for nuclear power plants, instructions refer to “nuclear generation emergency management”

# Crisis Management

## Critical event definition





# Crisis Management

## Classification of critical event

### Red Code(\*)

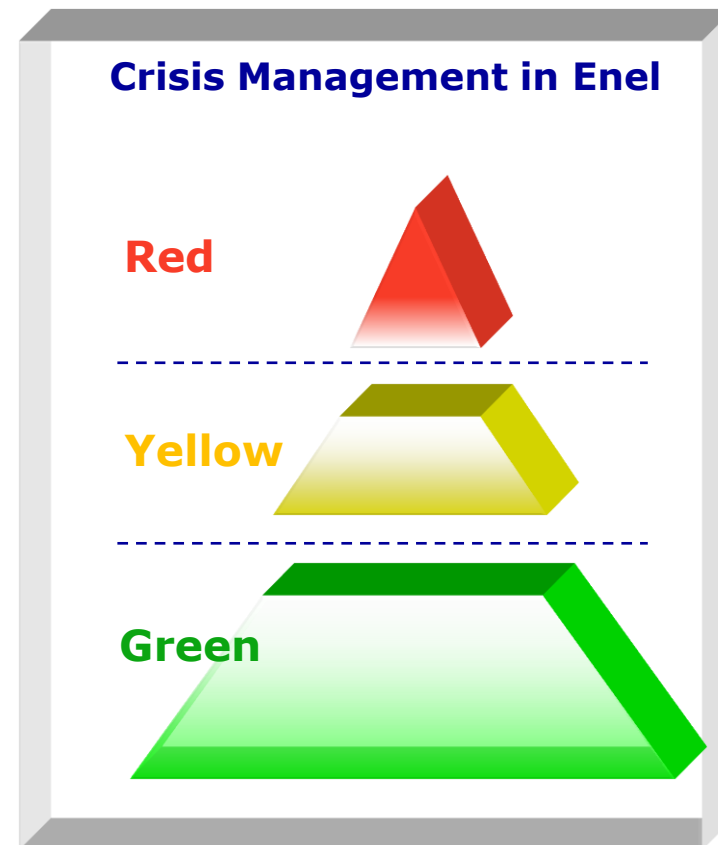
omissis

### Yellow Code

omissis

### Green Code

omissis



Impact level (green, yellow, red) is also evaluated using a Business Impact Analysis methodology (BIA)

An impact matrix has been defined to support the analysis of critical event (identification of threshold values for each type of event)

# Crisis Management

## Impact Matrix

Event	Impact level		
	Low <sup>(1)</sup>	Medium <sup>(2)</sup>	Relevant <sup>(3)</sup>
Distribution Electricity Network blackout			
Distribution Gas Network blackout			
Thermoelectric power plant inefficiency			
Hydroelectric power plant inefficiency			

1. local operating management of the event
2. local operating management of the event and constantly reports to Corporate Security, which activates the Joint Unit
3. strategic management of the event

# Crisis Management

## Impact Matrix

Event	Impact level		
	Low <sup>(1)</sup>	Medium <sup>(2)</sup>	Relevant <sup>(3)</sup>
Damage to Buildings			
Data Center unavailability			
Telecommunication Network unavailability			
Security Operation Center unavailability			
IT unavailability			
Customer Service inefficiency			
Natural (eg. earthquake, flood)			

1. local operating management of the event
2. local operating management of the event and constantly reports to Corporate Security, which activates the Joint Unit
3. strategic management of the event

# Crisis Management

## Impact Matrix

Event	Impact level		
	Low <sup>(1)</sup>	Medium <sup>(2)</sup>	Relevant <sup>(3)</sup>
People damage (employees and contractors)			
Pandemic			
<b>Malicious/Intentional events</b>			
Socio-political events (eg. coup d'etat, war)			
Damage to reputation			
Environmental damage			

1. local operating management of the event
2. local operating management of the event and constantly reports to Corporate Security, which activates the Joint Unit
3. strategic management of the event

## Sala Situazione Security

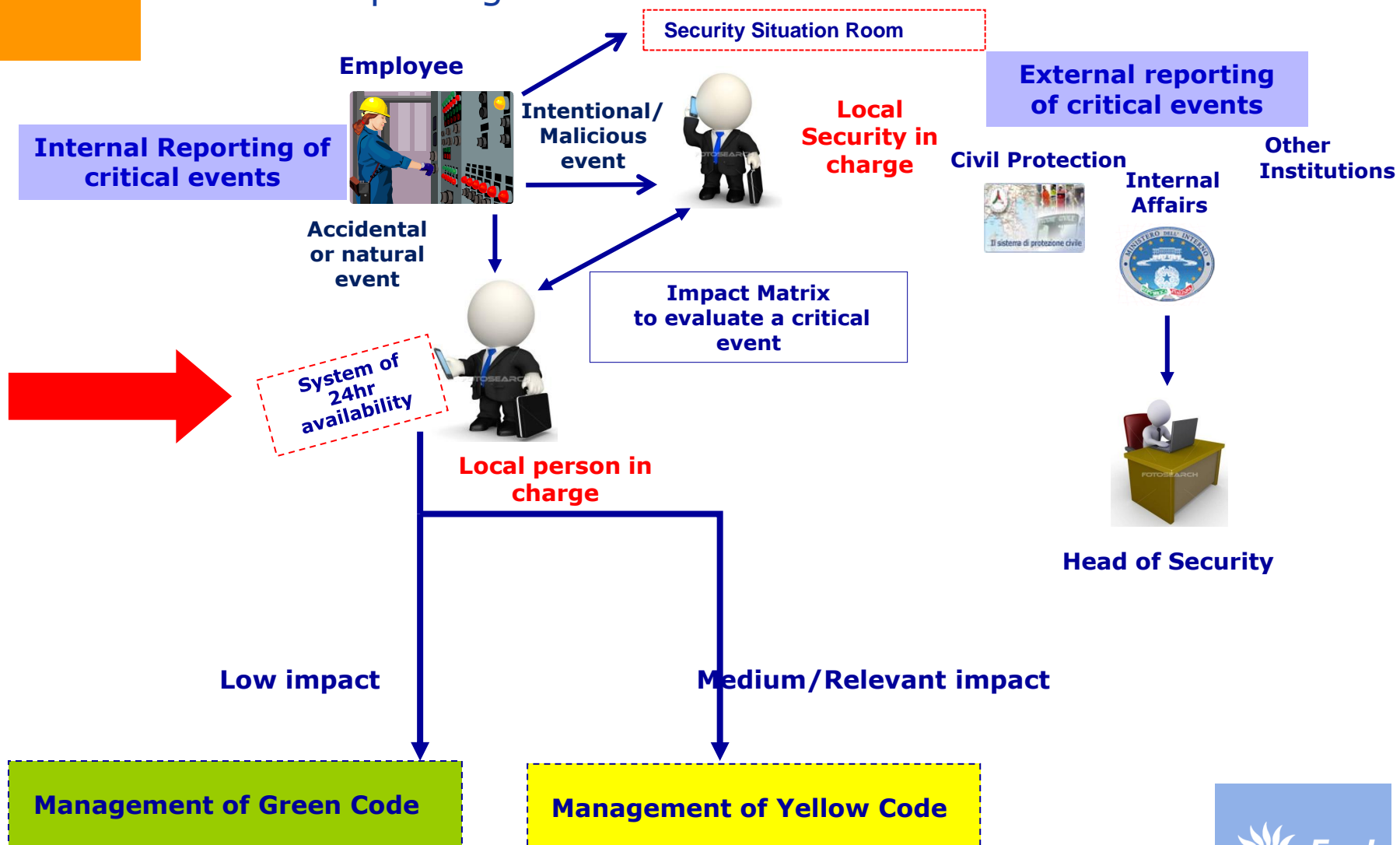
The Situation Room constitutes the main structure for:

- Security standard and protection systems
- Monitoring of the security early warnings
- Risk assessment, central and local unit alerting
- Activation of site security plans
- Information processing and reporting
- Relations with national security agencies



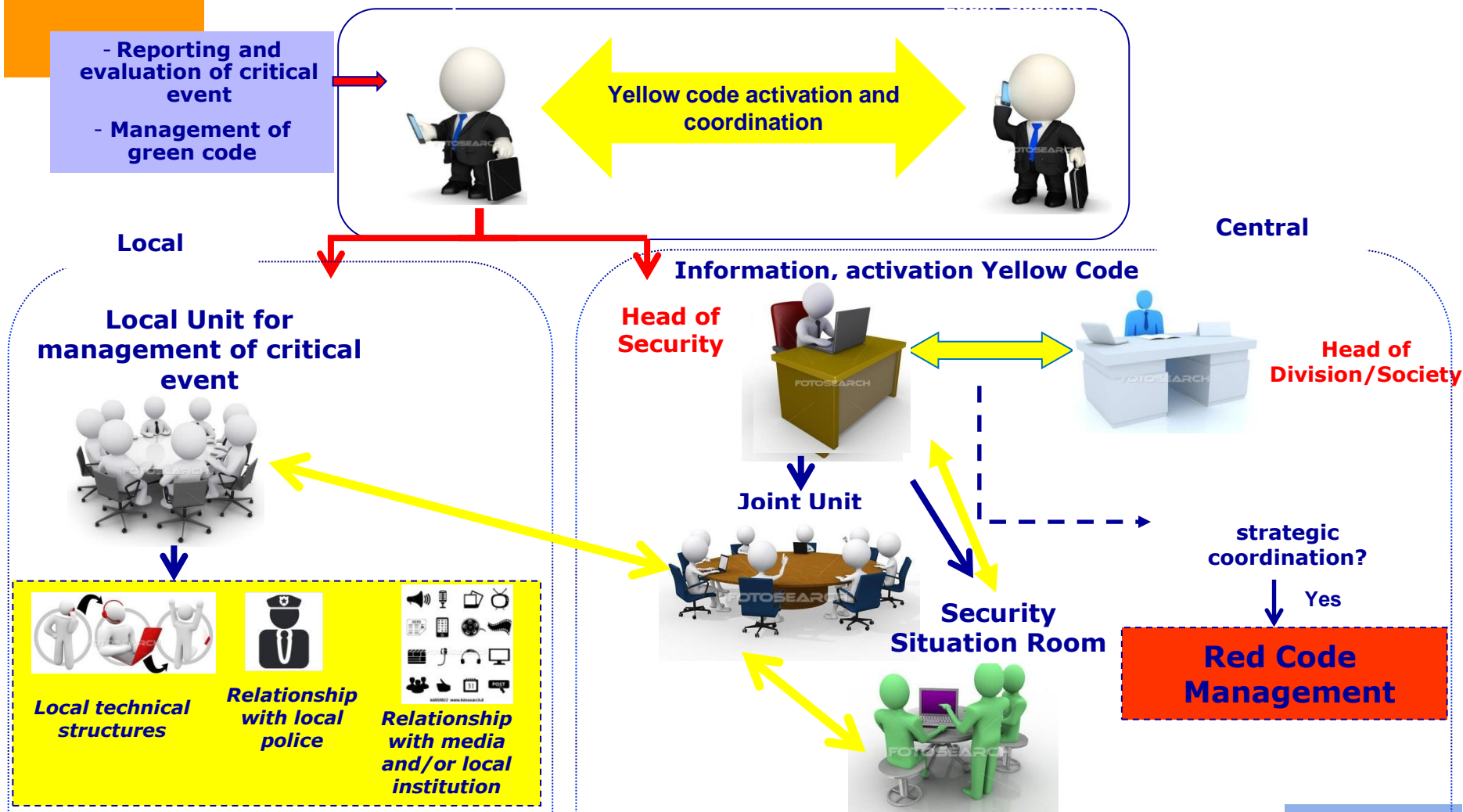
# Crisis Management

## Critical event - Reporting and Evaluation



# Crisis Management

## Critical event management- Yellow Code



# Crisis Management

## Critical event management - Red Code

