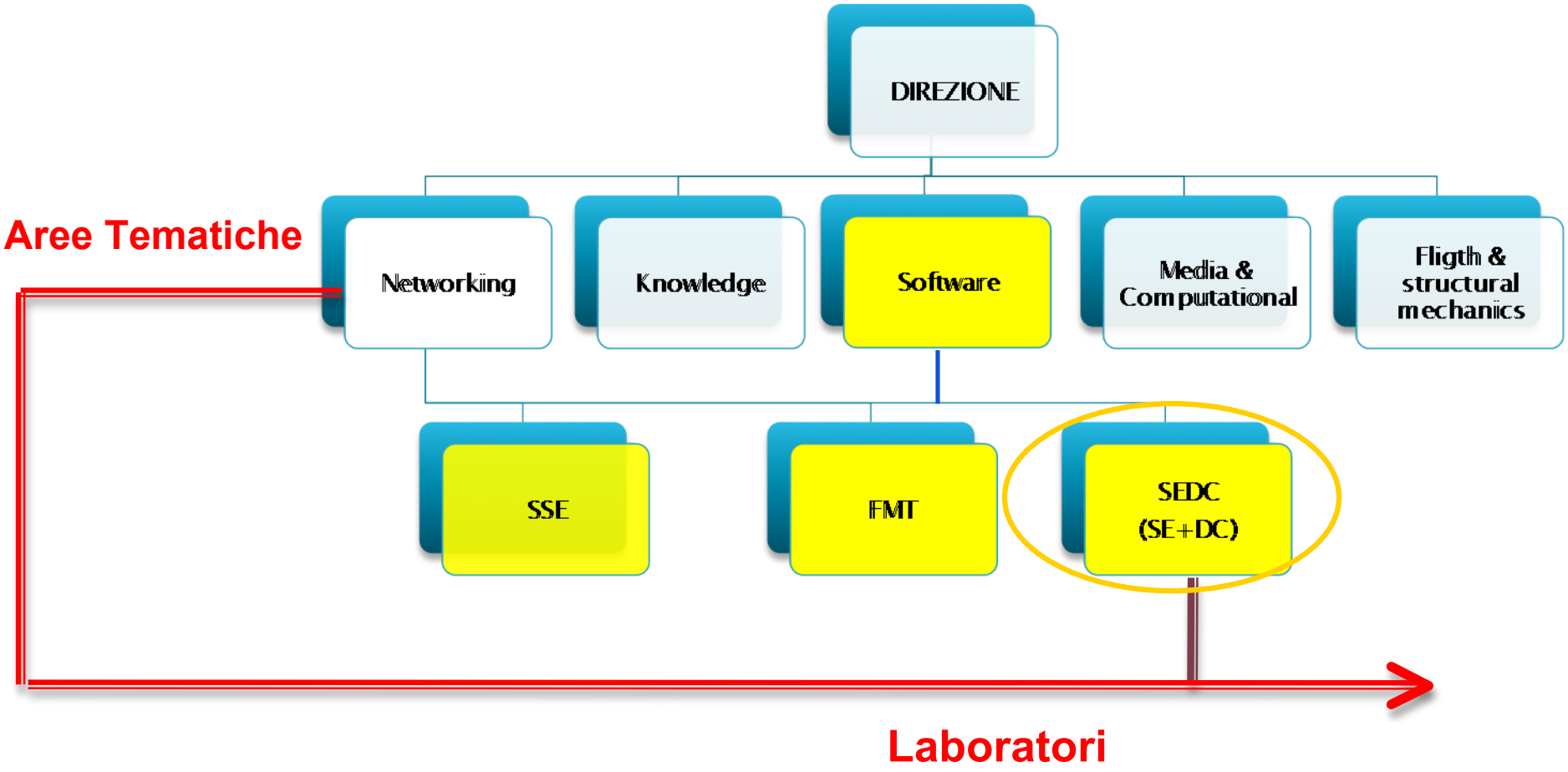
# Problematiche di Interdipendenze in Infrastrutture Critiche

Felicita Di Giandomenico
ISTI-CNR, Pisa
digiandomenico@isti.cnr.it

Seminario “ Logistica e ICT”
Livorno 02/03/2012

ISTITUTO DI SCIENZA E TECNOLOGIE
DELL’INFORMAZIONE “A. FAEDO”

# L'organizzazione ISTI



# Ricerca su Dependability all'ISTI

**Dependability:** proprietà di un sistema di calcolo per cui può essere riposta fiducia, in modo giustificato, nel servizio che esso offre

**Attività di Ricerca:**

- **Architetture/Meccanismi/tecniche per tollerare guasti durante la vita operativa del sistema**
  - ***Focus su adattività, flessibilità, eterogeneità***
- **Analisi quantitativa di indicatori di Dependability and QoS, mediante approcci probabilistici**
  - ***Supporto per effettuare scelte di progettazione, settaggio di parametri, raffinamento di soluzioni***
  - ***Stimare livelli di dependability/QoS di sistemi già costruiti***

**Condotta nel contesto di progetti di ricerca cooperativi, sia Europei che Nazionali**

# Infrastrutture Critiche

- **Organizzazioni** e **strutture** di **vitale importanza** per la società e dal cui **fallimento** o **interruzione** possono derivare conseguenze drammatiche
- **Molti settori coinvolti:**
  - Trasporti e Traffico
  - Finanza, fondi e assicurazioni
  - Governo, amministrazione e giustizia
  - Energia
  - Infrastruttura idrica
  - Materiali pericolosi
  - Telecomunicazioni
  - Information technology
  - Sanità
  - …

# Evoluzione delle condizioni operative di CI

- In passato:
  - Le infrastrutture potevano essere attaccate solo localmente
  - Interdipendenze limitate, solo a livello nazionale
- Oggi:
  - Forti relazioni all'interno e tra settori, attraverso infrastrutture ICT
  - Relazioni nazionali e transnazionali
  - Cooperazione nella fornitura di servizi
- In futuro:
  - Aumento dei disturbi di larga scala e della varietà delle minacce
  - Incidenti all'estero possono diventare un problema per la sicurezza interna
  - ……

# Iniziative per proteggere le infrastrutture

- Evidenza di fallimenti catastrofici nell'ultimo decennio
- La protezione delle CI nazionali è una priorità per molti Paesi
- Iniziative di ricerca promosse a livello Nazionale e Internazionale
  - Progetti promossi dalla EU (CRUTIAL, IRRIIS, GRID, ..) e da NSF (TCIP, ..)
- Creazione di Istituti e Organismi Internazionali
  - The International Institute for Critical Infrastructures - CRIS
  - IFIP Working Group 11.10 on Critical Infrastructure Protection
  - The Institute for Information Infrastructure Protection (The I3P)
  - ….

# Linee guida alla protezione di CI in ambito ICT

- Necessità di:
  - Progettazione seguendo principi rigorosi di ingegneria del software
  - Protezione contro guasti accidentali e attacchi intenzionali
  - Valutazione della resilience/trustworthiness
- Concetto di "Infrastructure Resilience"
  - Capacità di ridurre l'entità e/o la durata di eventi di fallimento/interruzione. L'efficacia di una infrastruttura "resiliente" dipende dalla sua capacità di *prevedere, assorbire, adattarsi a, e/o recuperare rapidamente* da un evento potenzialmente catastrofico

# Interdipendenze

**Definizione:**

relazione  bidirezionale tra due infrastrutture, attraverso cui lo stato di ciascuna infrastruttura  influenza o è correlato allo stato dell'altra. Più in generale, due infrastrutture sono interdipendenti quando ognuna è dipendente dall'altra.

Le interdipendenze sono di vario tipo. Le 4 principali sono: fisico, **cyber**, geografico e logico

Interdipendenza cyber: una infrastruttura dipende dall'informazione trasmessa da una infrastruttura informatica

# Esempi di interdipendenze tra infrastrutture

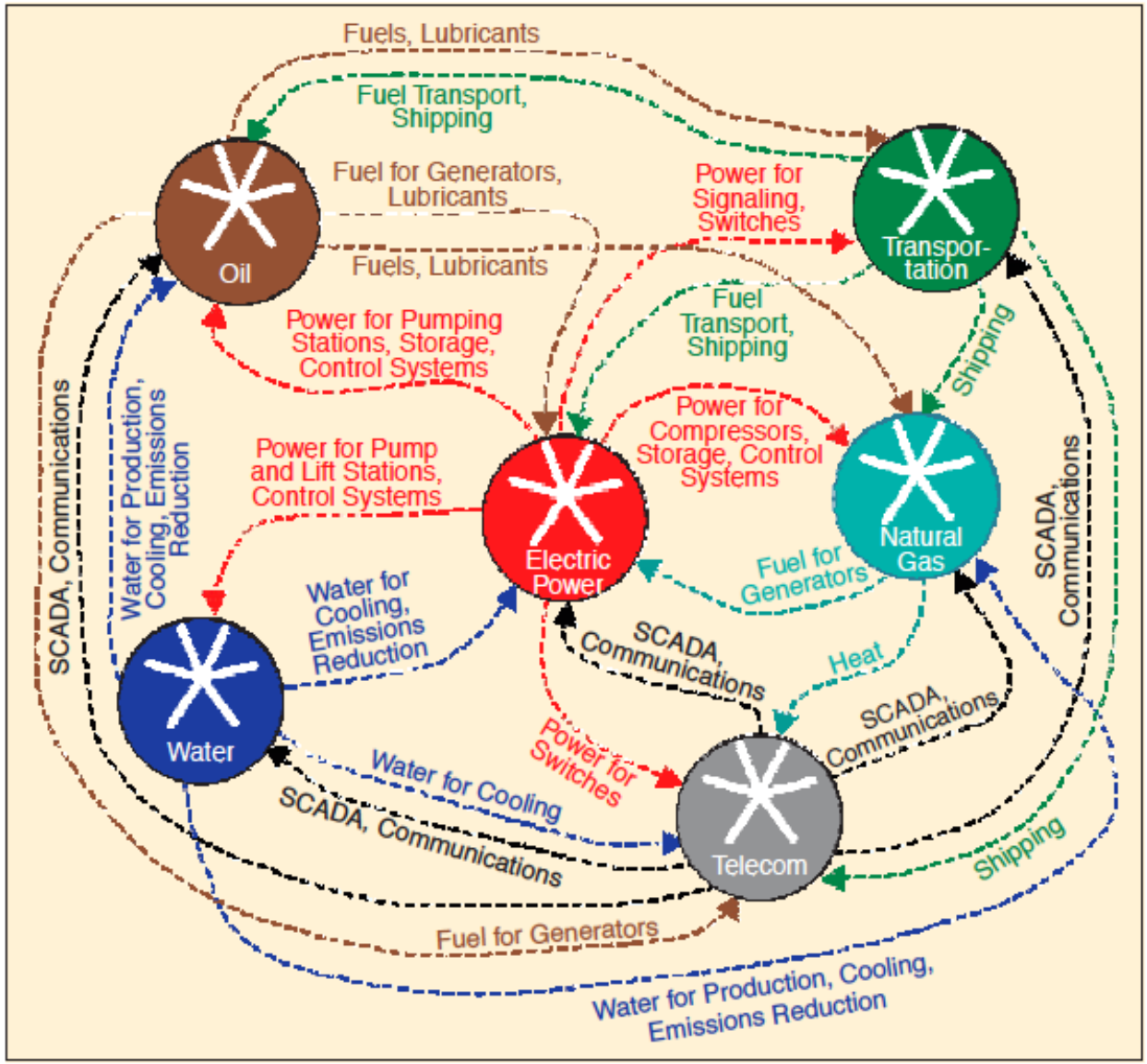


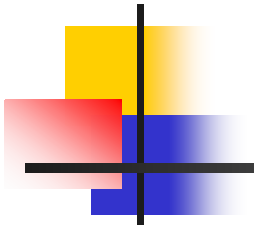

**Figure 3.** *Examples of infrastructure interdependencies.*

Estratto da:
S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. **Identifying, understanding, and analyzing critical infrastructure interdependencies**. IEEE Control Systems Magazine, pages 11-25, December 2001.

# Problemi causati da interdipendenze: alcuni esempi in ambito power grid

- Blackout Italiano del 28/09/2003:
  - “trip”della linea elettrica Mettlen-Lavorgo (Svizzera),
  - causando overloading su altre linee
  - causando il trip di altre linee e il blackout a livello nazionale
  - Forte dipendenza tra power network e communication network: l’indisponibilità della rete elettrica ha casato indisponibilità di alimentazione dei dispositivi di comunicazione/controllo
- Blackout in Nord America del 14/08/2003
  - Problemi nella fornitura di potenza negli stati di Ohio e Indiana
  - in contemporanea, non operatività del “Midwest ISO state estimator and real-time contingency analysis software” che non permise “early warning assessment”
  - Il blackout risultante dalla mancanza di azioni di ripristino in tempo reale ha avuto impatto su 50M di persone in 8 stati USA e 2 province canadesi

# L'esperienza nel contesto del progetto EU CRUTIAL

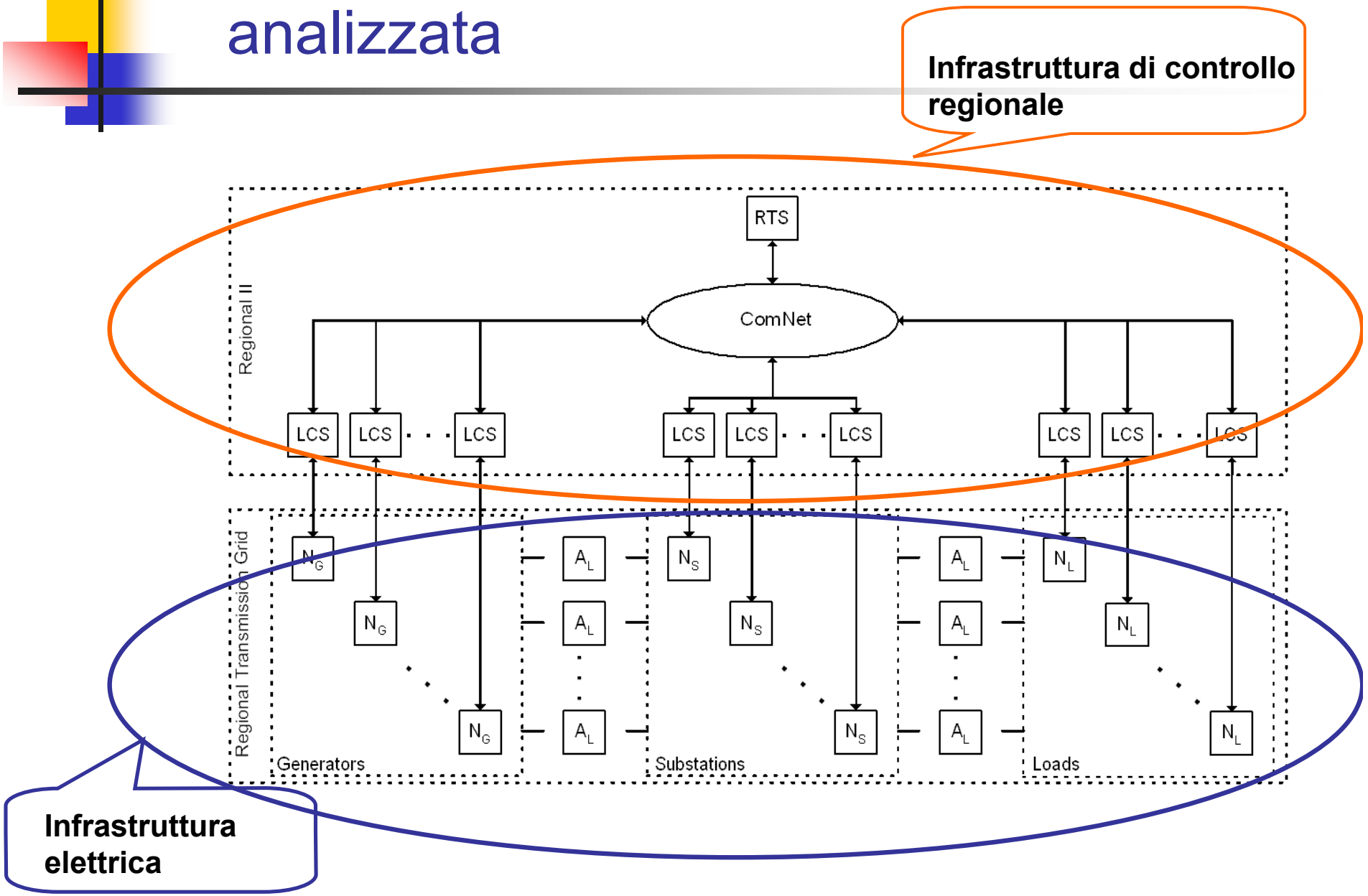


- Progetto STREP "CRitical UTility InfrastructurAL Resilience" (2006-2009)
- Due obiettivi principali:
  - Sviluppare approcci basati su modellazione per capire e controllare le varie interdipendenze tra le infrastrutture di potenza, di controllo e di comunicazione
  - Investigare architetture distribuite per il controllo e la gestione affidabile della griglia di elettrica

# Obiettivo

- Definizione di un **framework per la modellazione** capace di caratterizzare  e analizzare le interdipendenze tra le due infrastrutture del sistema elettrico (EPS)
  - L' infrastruttura di controllo
  - L' infrastruttura elettrica
- Focalizzado su **fallimenti correlati alle interdipendenze**:
  - Fallimenti "Cascading"
  - Fallimenti "Escalating"
  - Fallimenti "Common-cause"
- Obiettivo: stima quantitativa del loro impatto sulla resilence di queste infrastrutture
- **Framework di valutazione generale**, popolato di building blocks che rappresentano eventi base, componibili per rappresentare potenzialmente una qualsiasi configurazione di EPS

# Struttura Logica dell'Istanza di EPS analizzata



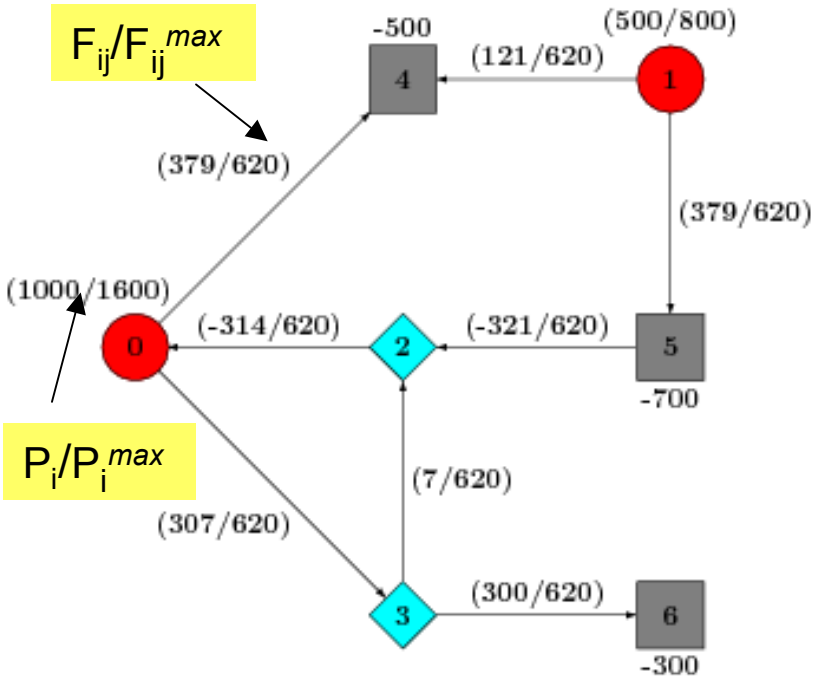
# Misure di interesse

- Misure rappresentative del buon funzionamento del sistema per l'utente
  - **Percentuale attesa** di potenza non erogata a un certo tempo t o in un intervallo di tempo [0, t]
- Misure rappresentative del buon funzionamento del sistema per il fornitore del servizio
  - **Guadagno** atteso al tempo t o in un intervallo [0,t], calcolato su una struttura di guadagno, in cui costi sono associati a generatori e a interruzioni di servizio, e guadagni sono associati a utenti soddisfatti, …
  - **Numero atteso** di componenti colpiti da un disservizio al tempo t o in un intervallo [0,t]

# Tipi di analisi

- Analisi dell'evoluzione dello stato della griglia elettrica in seguito ad eventi di fallimento, utile per
  - Tracciare la propagazione del fallimento ed eventi correlati nel tempo
  - Validare il metodo e i modelli in situazioni ben circoscritte
- Analisi per identificare le linee elettriche critiche e stimare gli effetti di scenari di fallimento su indicatori correlati al blackout, utile per
  - Comprendere l'impatto relativo di  processi di fallimento/riparazione e la criticità degli elementi del sistema elettrico

# Evoluzione dello stato del sistema elettrico




2 Generators (red)
2 Substations (cyan)
3 Loads (gray)
8 Power lines

## Fallimenti considerati:

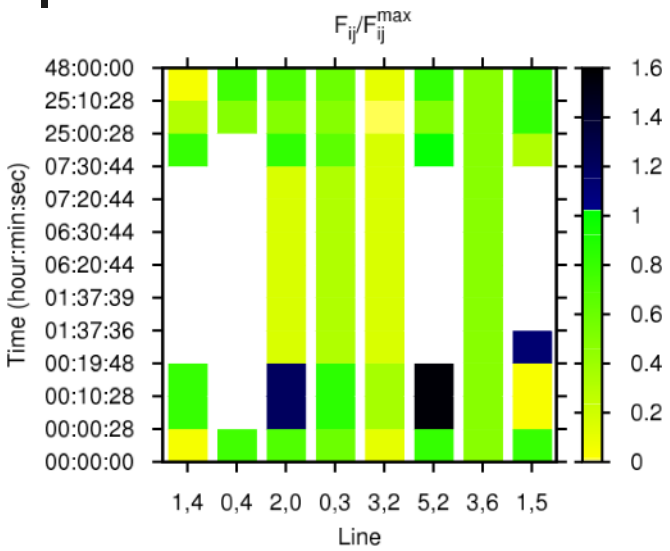
- fallimento permanente della linea (0,4)
- fallimento di omissione della rete di comunicazione (ritardo nell'applicare la riconfigurazione)

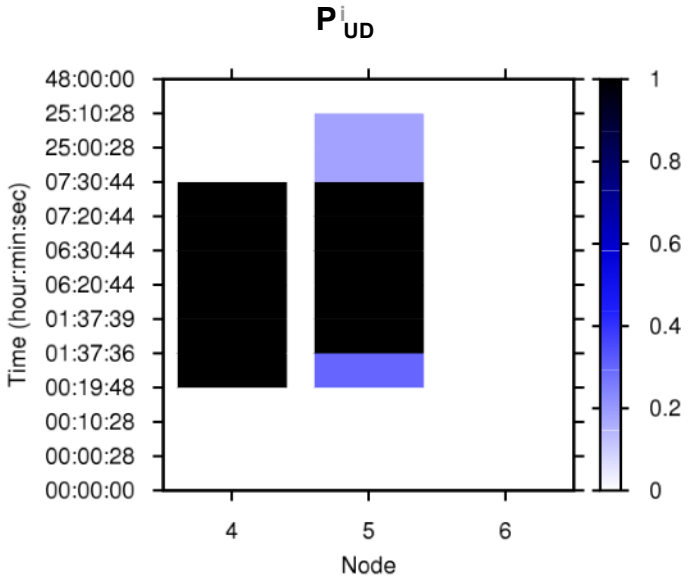
## Intervallo temporale considerato: 48 ore

$F_{ij}^{max}$= 620 MW per ogni i,j

Misura calcolata: $\mathbf{P^{i}_{UD}(t)}$ percentuale di energia non erogata al carico j

# Alcuni risultati

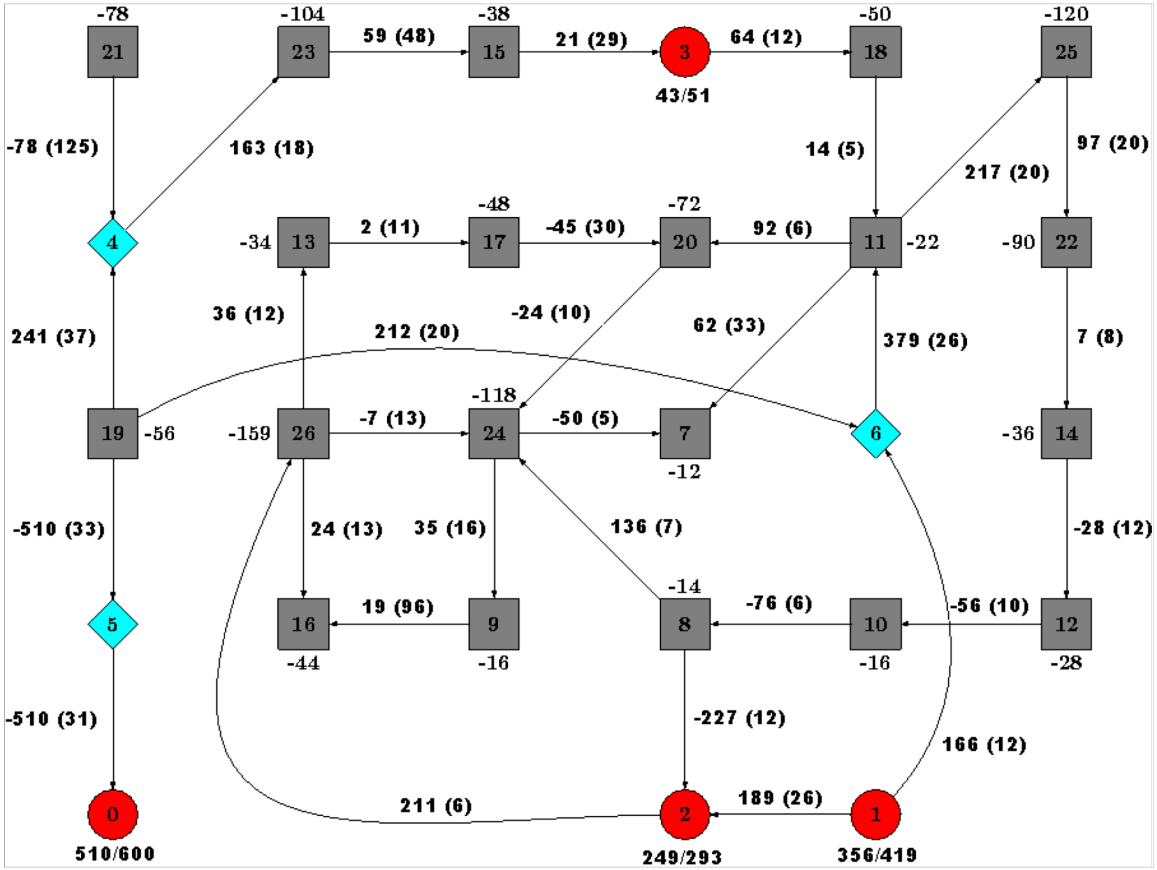



- **bianco** indica flusso di potenza zero
- **valori >1** (barra colorata a dx) indicano livelli di sovraccarico

- **barra colorata** rappresenta la percentuale di carico non soddisfatto
- **bianco** indica che la richiesta di carico è pienamente soddisfatta, **nero** l'opposto

# Impatto di fallimenti nella rete e nel sistema di controllo



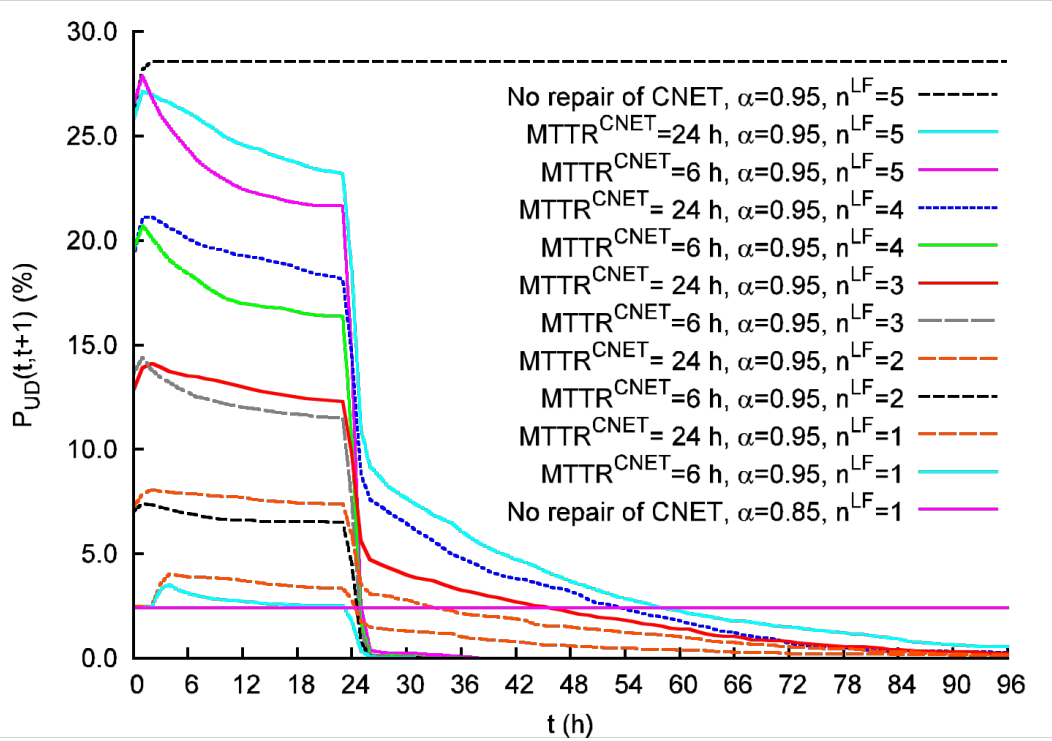

Maximum power flow through the lines = 620 MW

Diagramma della griglia elettrica EI (una porzione del IEEE 118 Bus Test Case)

# Scenario analizzato

- Al tempo zero, **$n^{LF}$ linee elettriche diventano simultaneamente indisponibili per un fallimento permanente** (e.g., per la caduta di un albero o un attacco terroristico).
  - Le linee fallite vengono riparate dopo 24 ore.
- Al tempo zero, **ComNet è affetta da un attacco DoS**.
  - L'indisponibilità della rete di comunicazione non permette di attuare riconfigurazioni della rete elettrica da parte del controllo
  - L'attacco DoS termina dopo un tempo di riparazione (distribuito *esponenzialmente)* permettendo quindi il ripristino della rete elettrica.
- **Misura di Interesse**: *percentuale della richiesta di potenza non soddisfatta in [t,t+1]* ore

# $P_{UD}(t,t+1)$ ,con t=0,1,…,96 ore, per differenti valori di $MTTR^{CNET}$ (6,24 h.) e $n^{LF}$ (1,…,5)




- $P_{UD}(t,t+1)$ aumenta considerando valori più alti di $n^{LF}$, e fissando il valore per $n^{LF}$, $P_{UD}(t,t+1)$ peggiora per attacchi DoS di maggiore durata (24 ore).
- Dopo 24 ore, la linea danneggiata è riparata, e conseguentemente $P_{UD}(t,t+1)$ decresce rapidamente fino a raggiungere il valore 0.

# (Alcune) Raccomandazioni (da rapporto NIAC, 2009)

- La “resilience” è una dimensione fondamentale delle CI
- Metodi e tecniche per aumentare la capacità di previsione, assorbimento, adattamento e rapido ripristino da un evento potenzialmente catastrofico sono necessari, e.g.:
  - *La capacità di previsione può essere migliorata attraverso analisi preventive dell’impatto di malfunzionamenti*
  - La capacità di assorbimento mediante uso di ridondanza
  - L’adattività è ottenibile attraverso un uso efficace delle risorse disponibili
  - Il rapido ripristino attraverso la minimizzazione dei tempi di riparazione

- Bilanciamento costi - robustezza
  - > robustezza ⟹ > costi per realizzarla

    ma anche
  - > robustezza ⟹ < costi dovuti a indisponibilità del sistema

# (Alcune) Raccomandazioni (da rapporto NIAC, 2009)

- Avanzamenti nei sistemi di controllo industriali migliorano l'operatività del sistema, ma introducono vulnerabilità aggiuntive e aumentano le interdipendenze, i cui effetti sono difficili da rilevare e fronteggiare.
- Per rendere questi sistemi capaci di fronteggiare le minacce a cui sono esposti, è necessario integrare aspetti di:
  - **resilienza,**
  - **sicurezza,**
  - **interazione umana, e**
  - **progettazione di reti complesse**
- Ma anche
  - migliorare la risposta al disastro e gli sforzi per il recupero attraverso il miglioramento della cooperazione e la condivisione di informazioni tra gli attori coinvolti - necessità di politiche inter-governative adeguate

# References


- Chiaradonna S., Di Giandomenico F., Lollini P. Interdependency analysis in electric power systems. In: Critical Information Infrastructures Security. pp. 60 - 71. Roberto Setola, Stefan Geretshuber (eds.). (Lecture Notes in Computer Science, vol. 5508). Berlin/Heidelberg: Springer Verlag, 2009.
- Chiaradonna S., Di Giandomenico F., Lollini P. Evaluation of critical infrastructures: challenges and viable approaches. In: Architecting Dependable Systems V. pp. 52 - 77. Rogerio de Lemos, Felicita Di Giandomenico, Cristina Gacek, Henry Muccini, Marlon Vieira (eds.). (Lecture Notes in Computer Science, vol. 5135). Germany: Springer, 2008.
- S. Chiaradonna, F. Di Giandomenico, P. Lollini, Definition, implementation and application of a model-based framework for the analysis of interdependencies in electric power systems, International Journal of Critical Infrastructure Protection (IJCIP) 4 (1) (2011) 24–40.
- Romani F., Chiaradonna S., Di Giandomenico F., Simoncini L. Simulation models and implementation of a simulator for the performability analysis of electric power systems considering interdependencies. In: 10th IEEE High Assurance Systems Engineering Symposium. HASE'07 (Dallas, TX, 14-16 November 2007). Proceedings, pp. 305 - 312. IEEE Computer Society, 2007.
- S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, pages 11-25, December 2001.
- National Infrastructure Advisory Council, Critical Infrastructure Resilience - Final Report and Recommendations, September 2009.