ENTE PER LE NUOVE TECNOLOGIE, L'ENERGIA E L'AMBIENTE

Unità di Calcolo e Modellistica

Seminario di presentazione della ricerca e tesi svolta in ENEA, 2005-2006

L'ergonomia cognitiva e l'identificazione della vulnerabilità di organizzazioni umane: la prospettiva socio-cognitiva

Relatori: Pamela Sargeni

Adam Maria Gadomski

Facoltà di Scienze della Comunicazione "La Sapienza" di Roma, Cattedra di Ergonomia *Interazione uomo – macchina*

High-Intelligence & Decision Research Group

CAMO – ENEA – Casaccia – edificio C59 sala conferenze – 10 Maggio 2006

OBIETTIVI

Generali:

Analisi degli aspetti dell'*ergonomia cognitiva* coinvolti nei *processi decisionali* che influenzano in modo critico la *vulnerabilità* di *organizzazioni complesse.*

Modellazione di *sistemi socio-cognitivi* che gestiscono e proteggono infrastrutture critiche, o che sono chiamati a gestire incidenti/disastri tecnologici e ambientali.

Specifici:

Mostrare l'utilità dei concetti principali e meta-modelli di TOGA per la modellazione di vulnerabilità gestionali dei grandi disastri naturali e tecnologici usando 5 Casi Reali.

STRUTTURA DELLA RICERCA

PARTE TEORICA

- ✓ Concetti di Base
- ✓ Metodo: La Meta-Teoria TOGA

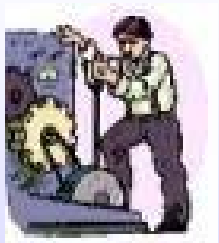
PARTE SPERIMENTALE

- ✓ Casi di studio
- ✓ Modellazione dei Casi
- ✓ Conclusioni
- ✓ Interviste 

PARTE TEORICA

1. Concetti di Base

- Ergonomia
- Organizzazioni Umane Complesse
- Vulnerabilità
- Processi Decisionali



CHE COS' E' L'ERGONOMIA

Termine coniato nel 1949 da F. H. Murrell per descrivere una disciplina che persegue la progettazione di prodotti, ambienti e servizi rispondenti alle necessità dell'utente.

….."Il lavoro deve essere organizzato in modo da rispettare le esigenze e i bisogni dell'uomo"…..

Oggi è una scienza interdisciplinare che coinvolge le conoscenze di diverse discipline: ingegneria, anatomia, biologia, fisiologia, adattando soprattutto gli strumenti di lavoro alle capacità fisiche del lavoratore.

Con lo sviluppo di complessi sistemi socio-tecnologici, vista l'enorme quantità di informazioni da valutare, si è reso indispensabile coinvolgere discipline quali la sociologia e la psicologia: nasce così l'"*ergonomia cognitiva*"

L'ERGONOMIA COGNITIVA

Ha come oggetto di studio l'interazione tra il *sistema cognitivo umano* e gli *strumenti* per l'elaborazione dell'informazione.

Due percorsi:

1. studio e progettazione dell'interazione uomo-computer (usabilità delle interfacce operatore - sistemi tecnologici);
2. studio delle funzioni cognitive dell'individuo e dell' organizzazione, e lo sviluppo di strumenti software per supportare diverse funzioni di ragionamento individuale e di gruppo.

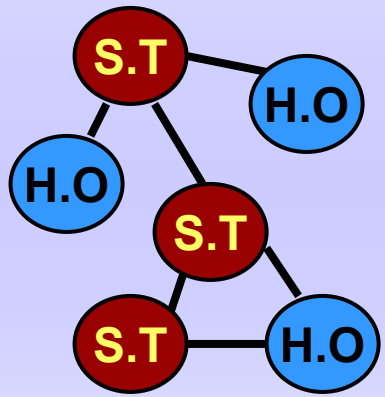
Questo secondo studio, nel contesto delle organizzazioni umane, *è* focalizzato sul *decision-making* soprattutto durante il controllo e la gestione di situazioni di alto rischio ed eventi imprevisti.

L'ergonomia cognitiva affronta i problemi di modellazione delle attività mentali dell'individuo nelle organizzazioni umane per ridurre la probabilità di errori umani, cercando di rendere l'interazioni ***uomo-organizzazione-dominio_di_attività*** *più* efficace e affidabile.

Che Cos'e' la Complessità Organizzativa?

È una proprietà delle grandi organizzazioni le quali sono inserite in una rete socio-tecnologica ed eterogenea composta da combinazioni di componenti umane, tecnologiche ed organizzative, strettamente interdipendenti finalizzate al raggiungimento degli stessi obiettivi.

Frame generico di concettualizzazione sistemica



Rete di Organizzazioni e sistemi tecnologici

H.O *Human Organization*

S.T *System technology*

Che cos'è la Vulnerabilità?

È la mancanza di immunità o l'insufficiente resistenza su un inaspettato ma possibile evento.

Vulnerabilità INTERNA: crisi interne, patologie di gestione e riorganizzazioni improprie.

Vulnerabilità ESTERNA: situazioni pericolose, attacchi, intrusioni, minacce umane, naturali tecnologiche e del mercato.

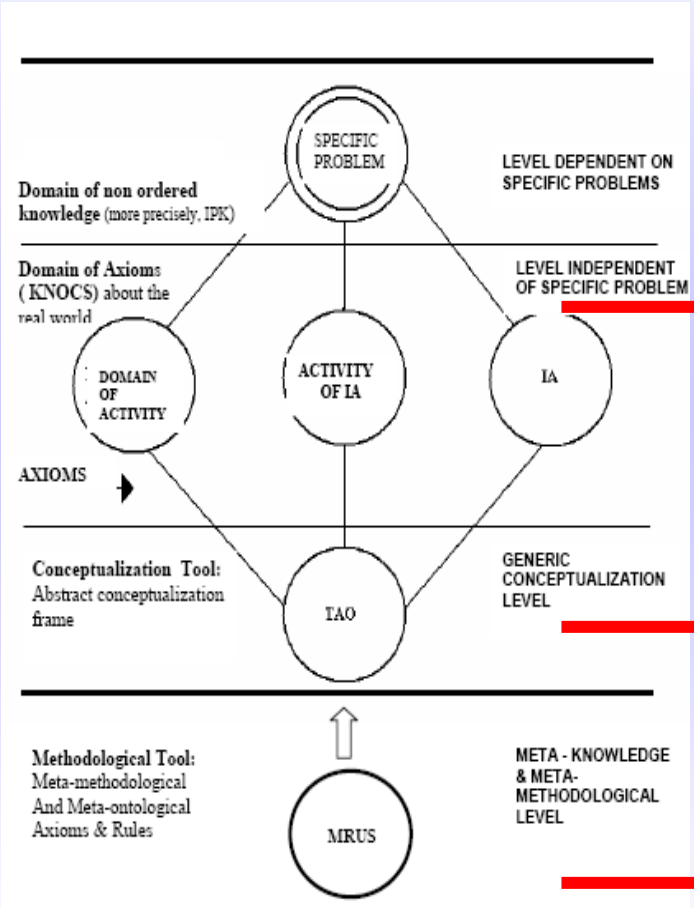
2. Metodo: TOGA *(Top-down Object-based Goal-oriented Approach)*

Meta-Teoria sviluppata per l'ordinamento della conoscenza relativa alla specificazione e gestione di problemi complessi(1990). La Teoria ha il merito grazie alla sua visione *Top down* e *Goal oriented* di partire da una visione generale del fenomeno per poi entrare gradualmente nei dettagli secondo un'*azione orientata all'obiettivo*.

Le 3 sotto-teorie che insieme concorrono alla sua formazione sono:

1. **TAO** "*Teoria degli oggetti astratti*"
2. **KNOCS** "*Sistema di concettualizzazione della conoscenza*"
3. **MRUS** "*Sistema di regole metodologiche*"

La Struttura TOGA



KNOCS

TAO

MRUS

Fornisce le basi per l'applicazione di TAO, ai problemi concreti e alle situazioni decisionali. Il fine di questa teoria è di descrivere l'interazione tra un *agente intelligente* ed il *mondo reale.*

Sistema di concettualizzazione per la rappresentazione della conoscenza indipendentemente dal *dominio di attività.*

È un approccio *Top-down* e *Goal-oriented* per l'ordinamento della conoscenza e la specificazione di problemi complessi.

In Cosa Consiste il Processo Decisionale?

È un'attività mentale implicita, di un individuo o di una struttura dei individui, che necessita di una scelta

- **Senza conoscere un criterio**
- **Senza conoscere le alternative**

Gadomski 1997

Decisioni individuali → la scelta ha una duplice valenza affettiva:

– Coniugazione *desiderio/bisogno*

– *Perdita*

Decisioni organizzative → coinvolgimento più di una persona, spesso più di un'organizzazione .

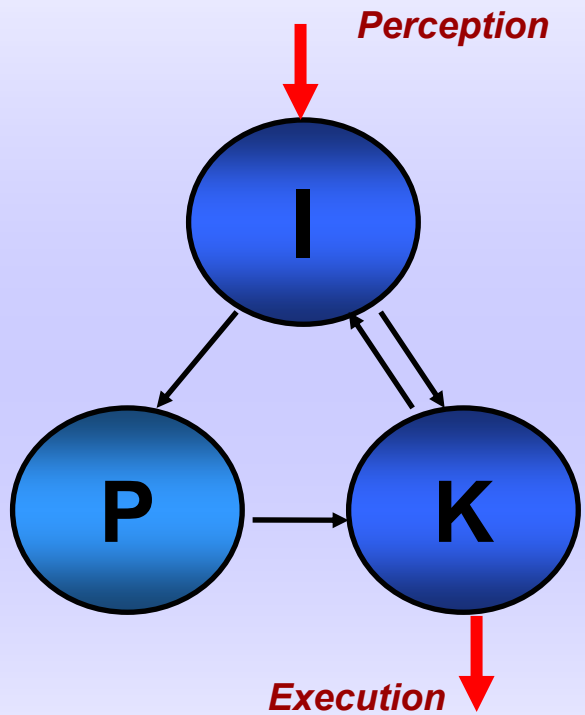
Dominio di interesse

L'ARCHITETTURA IPK

Informazioni: dati che rappresentano una proprietà specifica del dominio di attività dell'agente umano o artificiale (es. indirizzi, numeri di telefono, liste di nomi e misure

Preferenze*:* regole di relazione tra gli stati del *dominio di attività* dell'agente che indicano, in modo relativo, qual'è lo stato preferito (con maggiore utilità) tra due presi in considerazione. Le relazioni di preferenza servono per stabilire un (obiettivo di intervento) per un agente;

Conoscenze: ogni proprietà astratta di un agente in grado di processare informazioni in altre informazioni (es. istruzioni, procedure di emergenza, manuali, materiali scientifici, modelli, teorie…)



L'AGENTE INTELLIGENTE

"Un agente intelligente ha la capacità di modificare le sue stesse informazioni, preferenze, e conoscenze"

Gadomski 1997

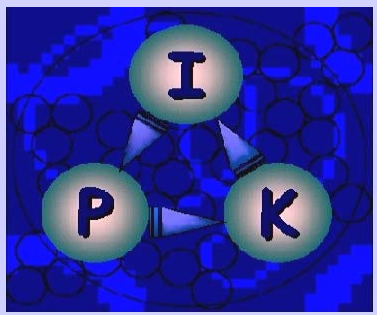
Ogni nuova informazione è processata dalla conoscenza:

$I_n' = K_{jn}(I_n)$, j=1, …J, per il dominio Δ ,

dove la scelta di K_j **dipende** dallo stato massimi preferito detto intervention goal:

max{ P (I_n)} == Intervention_Goal,

e **n** indica la concettualizzazione del punto di vista



Un **ASA**
Agente Semplice Astratto
viene chiamato
Monade

Una monade da sola NON può essere considerata un AI, più monadi possono essere organizzate gerarchicamente e costituire un agente intelligente.

IL PERSONOIDE

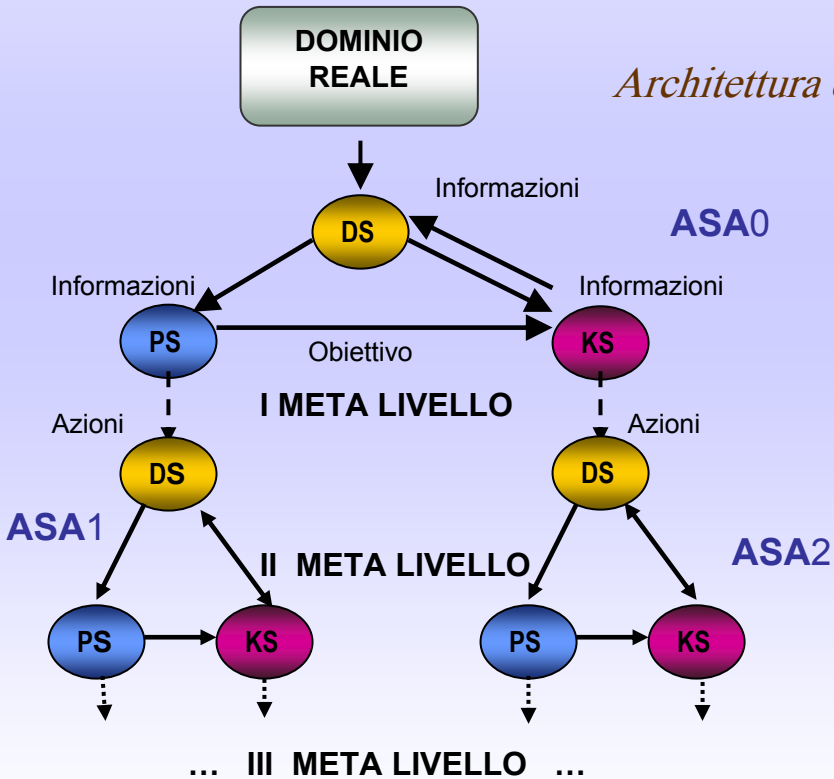
*"Il **personoide** rappresenta un'estrazione di funzioni della mente umana nella forma astratta, che può essere considerata come entità di base di ogni sistema intelligente guidato dagli obiettivi"*

Gadomski 1997

Per esempio

Se la Monade di I livello ASA0 non possieda le basi P e K sufficienti per definire un *goal* (la massima *preferenza)*, dovrebbe attivarsi, un'altra monade ASA1 di livello superiore per poter modificare la base di preferenze di ASA0 .

Architettura di un Personoide



Questa struttura è:

Frattale,

Ripetitiva

Ricorsiva

PARADIGMA UMP

Universal Management Paradigm

Completa le proprietà funzionali degli agenti intelligenti (naturali o artificiali), ed in particolare esplicita la loro realizzazione sotto forma di personoidi e di organizzazioni di personoidi.

Struttura

Funzionale

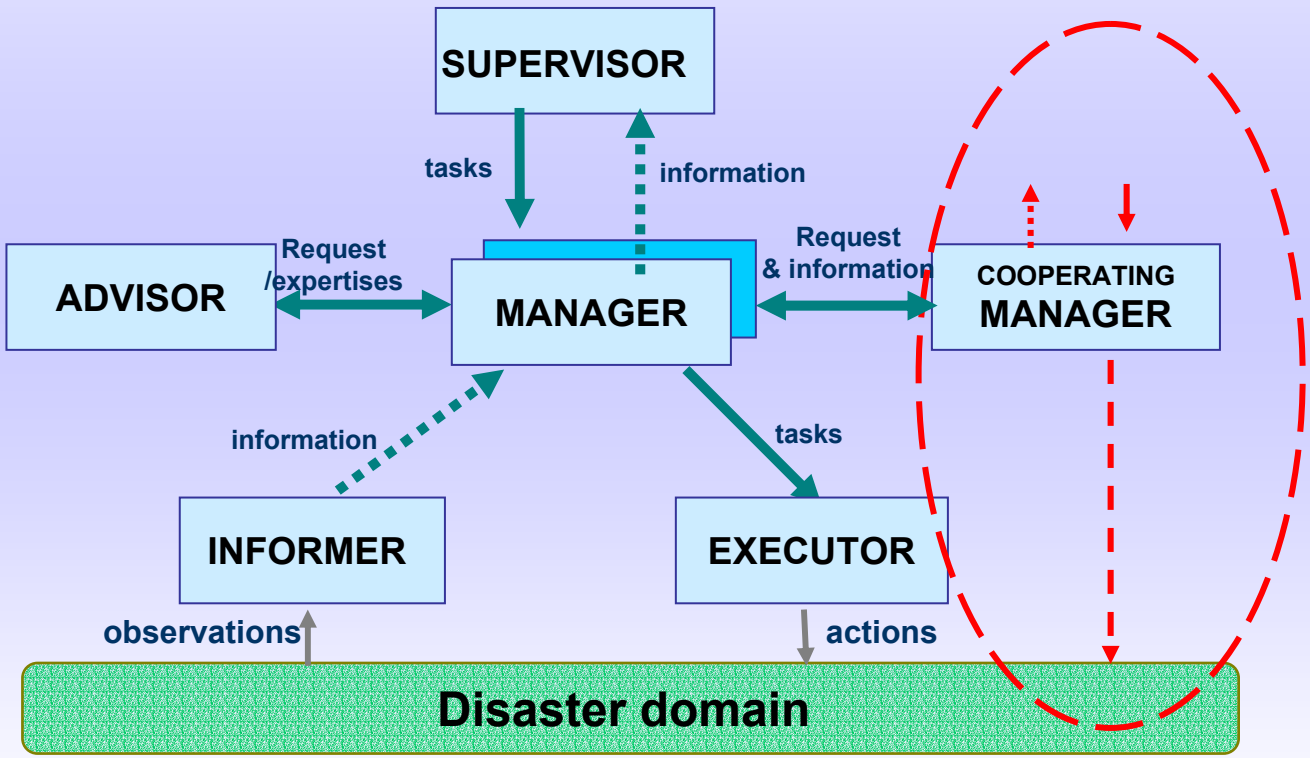
Completa

Modulare

Relativa

Ricorsiva

Incrementale

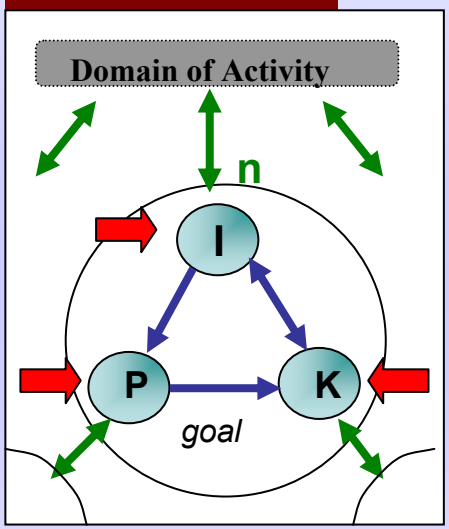


Rappresentazione di un processo decisionale semi-distribuito

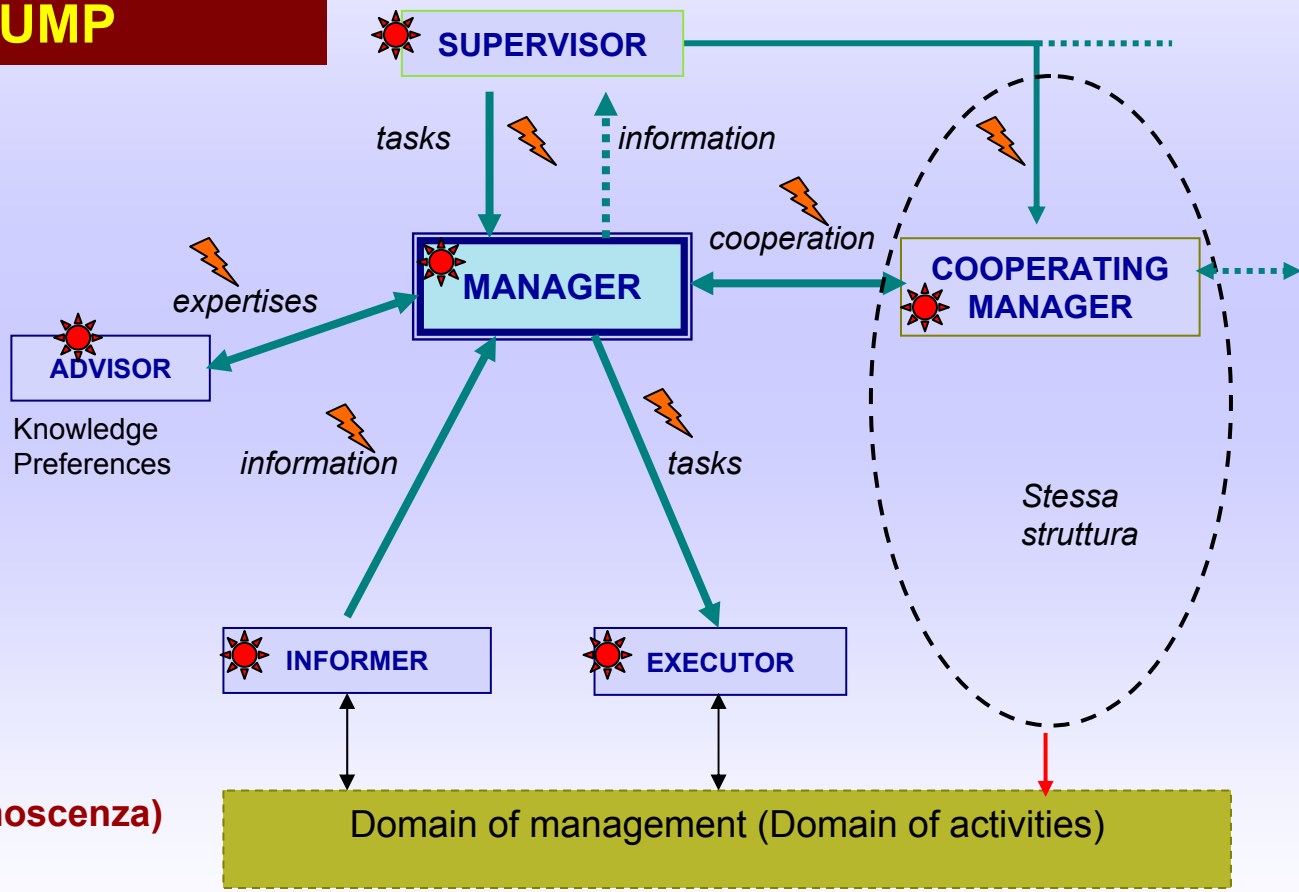
Ipotesi: Possibili Cause di Vulnerabilità Socio-Cognitive

[Gadomski, CNIP'2006]

IPK



UMP



Possiamo distinguere:

- **Informazioni insufficienti**
- **Preferenze improprie**
- **Competenze inadeguate (conoscenza)**
- **Comunicazione impropria**

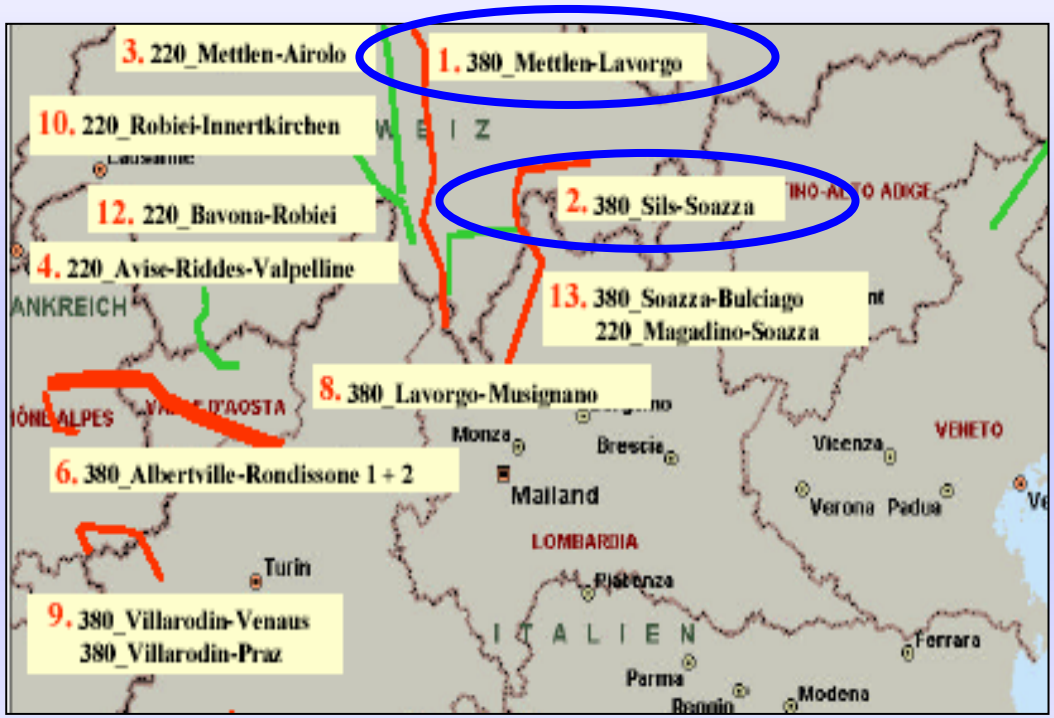
PARTE SPERIMENTALE

- Casi di studio
- Modellazione dei Casi
- Analisi dei Risultati
- Interviste
- Conclusioni Finali

Casi di studio

1. Il Blackout Italia/Svizzera del 28 settembre 2003
2. Il disastro di Chernobyl
3. L'uragano Katrina
4. L'incidente all'aeroporto di Linate
5. Tsunami: catastrofe nell'Oceano Indiano

1. Il Blackout Italia-Svizzera del 28 settembre 2003



Cronologia eventi:

03.01 in seguito ad una scarica tra un conduttore elettrico ed un albero si interrompe la linea c.d "Lucomanno" . Si verifica un sovraccarico sulla linea vicina c.d "San Bernardino";

03.11 Atel tenta inutilmente di ricollegare la linea del Lucomanno. Etrans contatta Grtn e gli chiede di correggere la differenza non programmata di 300KW per riportare al 100% il carico della linea del San Bernardino;

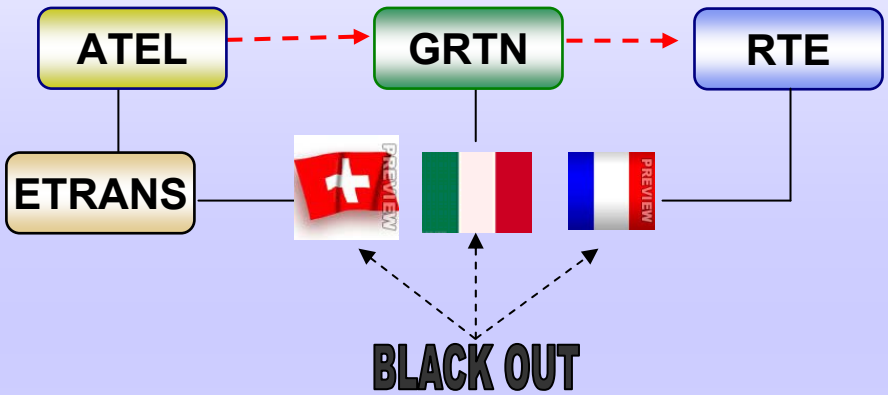
03.21 Grtn riporta il sistema italiano ai programmi concordati;

03.25 un cortocircuito verso terra sull'elettrodotto del S.Bernardino porta all'interruzione anche di questa linea.

Con la perdita di due linee importanti i sovraccarichi sulle altre linee rimaste in servizio nell'area diventano intollerabili, alle 03:27 si verifica l'interruzione a cascata di altre linee verso l'Italia.

BLACK OUT

Gestione dell'emergenza: due diversi punti di vista



P.D.V Svizzero ***"Non c'è stata alcuna lacuna di comunicazione"***

-esiste un collegamento informatico che trasmette in tempo reale in Italia i dati relativi all'import/export di energia

- a causare l'incidente sono stati l'eccesso di importazione di energia, e la scarsa reattività di Grtn

P.D.V Italiano ***"Ci sono stati gravi problemi di comunicazione"***

-Etrans non ha comunicato tempestivamente lo scatto della linea del Lucomanno;

-Il gestore svizzero si è limitato a denunciare un problema di riassetto interno, chiedendo al gestore italiano di limitare solo l'importazione dall'estero;

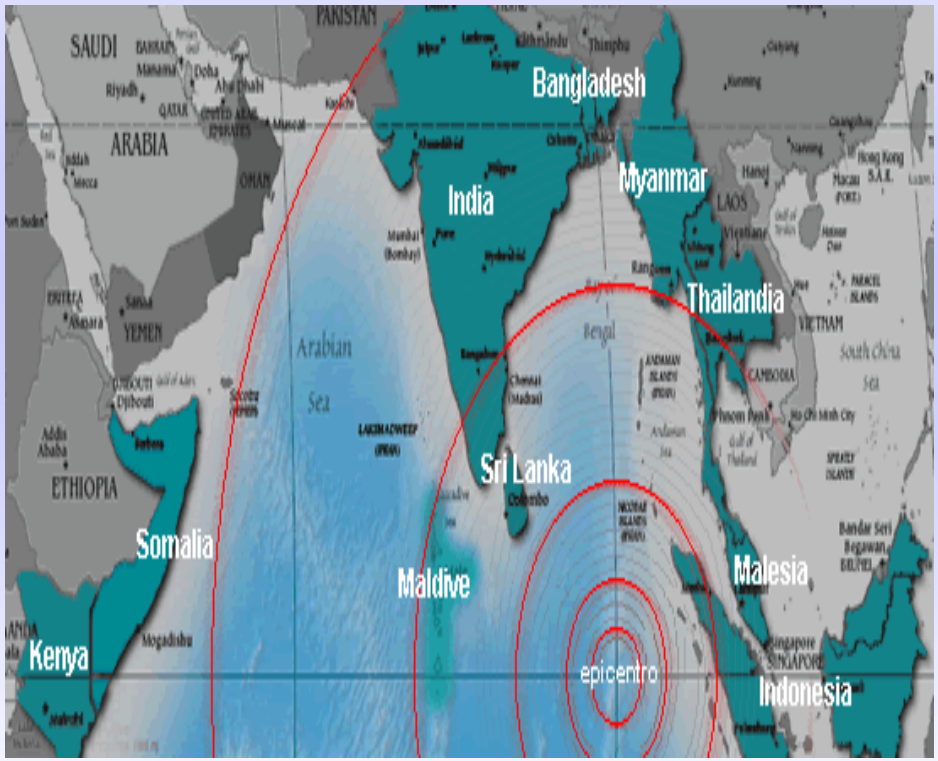
-Non ha adottato le procedure d'urgenza riguardanti le comunicazioni di stati di esercizio particolari;

Tabella Cause/Conseguenze

CAUSE	CONSEGUENZE
Condizioni esterne: cambiamento climatico, aumento della temperatura esterna	Aumento del fabbisogno energetico
Vulnerabilità progettuale*:* distanza insufficiente fra conduttori elettrici ed alberi	Scarica fra un conduttore elettrico ed un albero
Vulnerabilità progettuale: instabilità nella rete di Grtn	Difficoltà di gestione e di ripristino del sistema
Vulnerabilità operativa*:* sovraccarico della rete sulla linea di confine italia/svizzera	Fallimento nella riattivazione della linea del Lucomanno per eccessivo carico
Vulnerabilità operativa*:* tardiva attivazione delle misure di sicurezza	Perdita degli impianti di produzione e impossibilità per il sistema italiano di operare in modo isolato dalla rete UCTE.
Vulnerabilità organizzativa*:* Fallimento della comunicazione intra-organizzativa	I gestori della rete italiana e svizzera non riescono a coordinare gli interventi per il ripristino della rete elettrica

2. TSUNAMI: catastrofe nell'Oceano Indiano

Il 26 dicembre 2004 uno *tsunami* generato da un terremoto sul fondo del mare provoca uno spostamento nella zona delle isole Nicobare lungo una faglia di quasi 1000 metri. Lo spostamento causa un maremoto di enormi proporzioni.



Cronologia degli eventi:

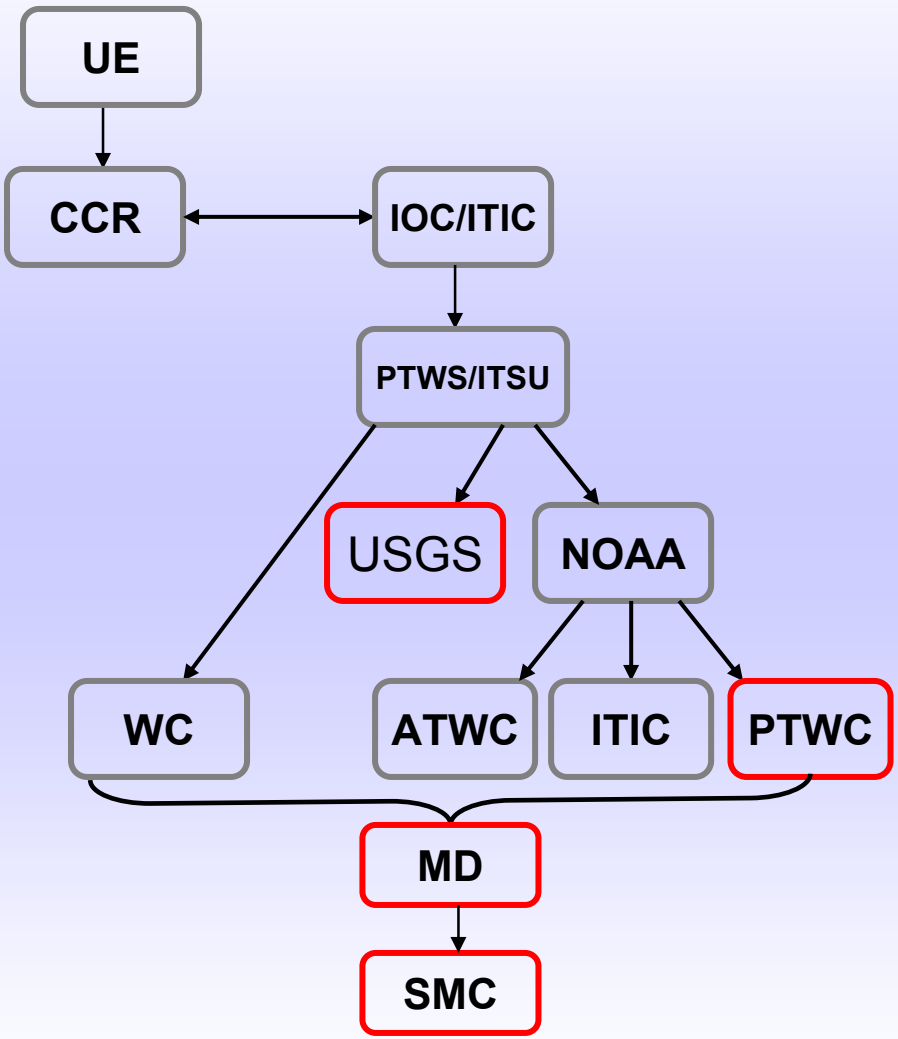
00:57 il terremoto di magnitudo 9 provoca lo spostamento della faglia causando il maremoto;

01:06 l'onda viaggia verso Sri Lanka e Thailandia;

03:02 raggiunge le Maldive;

12.00 c.a dopo quasi nove ore dalla prima scossa di terremoto, l'onda del maremoto raggiunge il Kenya. Si registrano "*onde anomale*" in tutto il mondo, dal Messico al Cile.

La gestione della comunicazione: cosa non ha funzionato?



Il terremoto viene registrato da 3 stazioni di monitoraggio USA:

1. **USGS→** non ha menzionato un possibile rischio tsunami al dipartimento di Stato americano, perchè non ha competenza per il monitoraggio dei maremoti;

2. **PTWC→**lancia un allerta generale nel Pacifico per poi smentire il tutto con un bollettino aggiornato inviato un ora dopo;

3. **ITIC→**viene contattato dal Ptwc, non diffonde l'informazione;

Il Ptwc non sa chi contattare, perde un ora prima di telefonare al centro meteorologico australiano, e lo fa quando ormai è troppo tardi per Sumatra, Sri Lanka, Thailandia, e la costa-est dell'India;

SMC Thailandia-Indonesia→ le informazioni in loro possesso sono discordanti. L'SMC thailandese da tempo non ha più contatti con il gruppo ITSU, non riceve i test mensili del PTWC

Tabella Cause e Conseguenze

CAUSE	CONSEGUENZE
Vulnerabilità tecnologica: assenza di un sistema di rilevamento tsunami nell'Oceano Indiano	Il terremoto non viene rilevato da nessun sistema locale di allarme
Vulnerabilità organizzativa: assenza di una rete di comunicazione tra i centri di rilevamento nazionali e le autorità locali	I centri di monitoraggio nazionali non diffondono la notizia di un possibile tsunami perché non hanno contatti aggiornati con le autorità locali
Vulnerabilità organizzativa: assenza di una rete di comunicazione tra le autorità locali	Anche a livello locale i centri di monitoraggio sismico non comunicano tra loro, l'allarme si limita a zone circoscritte
Vulnerabilità organizzativa: assenza di un organo di coordinamento locale	Le informazioni contraddittorie e non confermate contribuiscono a rallentare la pianificazione di un piano di emergenza
Vulnerabilità organizzativa: assenza di un piano di evacuazione	Caos sociale, fuga disordinata di masse terrorizzate

Modellazione dei Casi

Applicazione di TOGA

Top: Applicazione del **paradigma UMP** (*Universal Management Paradigm)* alla struttura organizzativa di ogni test case

Down: Applicazione dell'**architettura IPK** *(Information, Preferences, Knowledge)* ai ruoli identificati con il paradigma UMP.

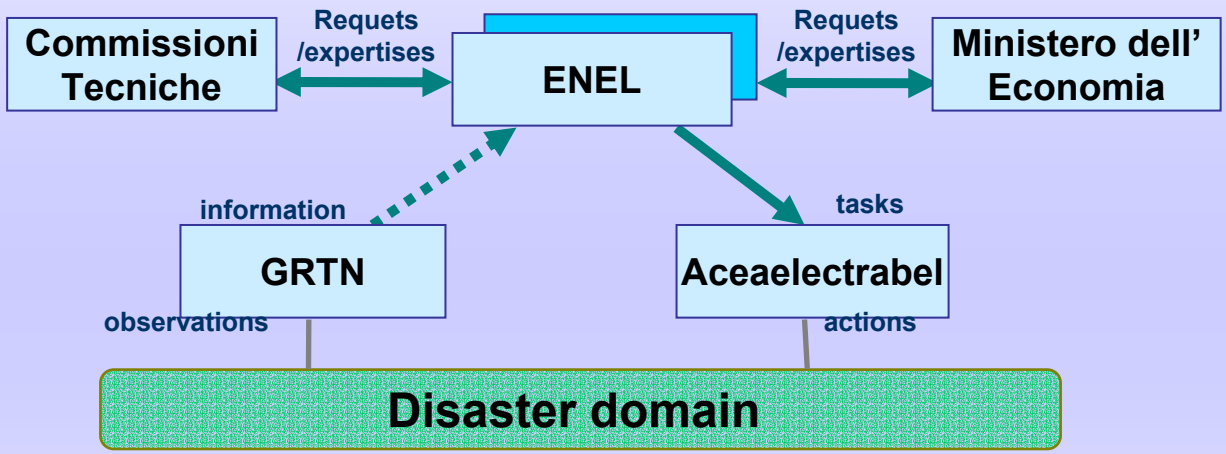
goal-oriented

Analisi della propagazione della vulnerabilità

1. Il Blackout Italia-Svizzera del 28 settembre 2003

SISTEMA ELETTRICO ITALIANO

Processo decisionale semi-distribuito

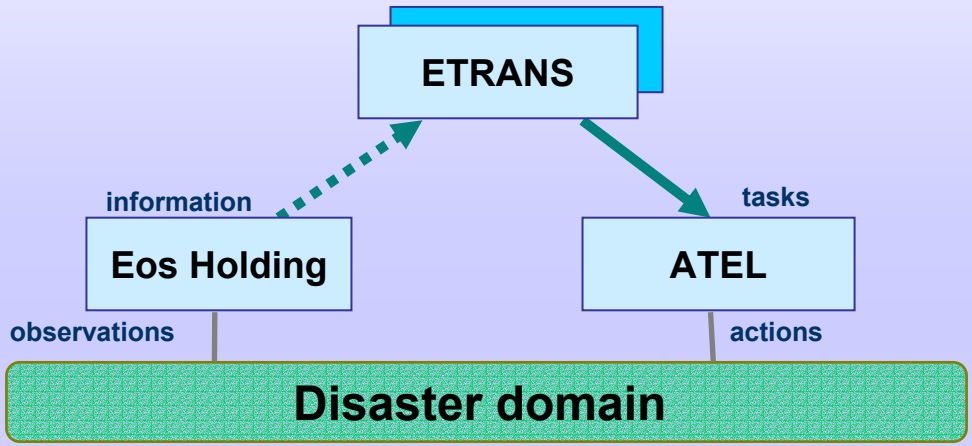


5 Ruoli:

1. **Manager** *"Enel" :" ha funzioni di indirizzo strategico e di coordinamento;*
2. **Advisor** *"Commissioni tecniche"* : forniscono consulenza in settori specifici del settore energetico;
3. **Cooperating manager** *"Ministero dell'Economia":* supporta l'ENEL nella definizione degli obiettivi strategici;
4. **Informer** *"Grtn"* : elabora mensilmente un Rapporto sul sistema elettrico contenente un'analisi sintetica del fabbisogno in energia ed in potenza;
5. **Executor** *"Aceaelectrabel"* :si occupa della generazione, vendita e commercializzazione di energia elettrica.

SISTEMA ELETTRICO SVIZZERO

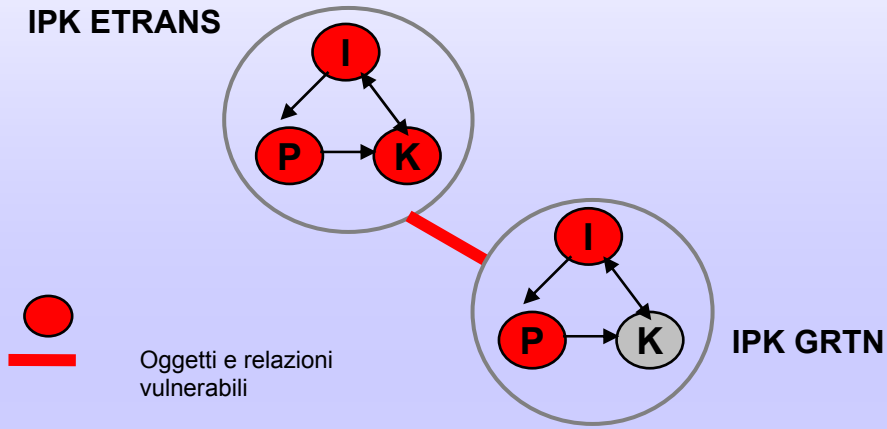
Processo decisionale centralizzato



3 Ruoli:

1. **Manager** "*Etrans*" : centro di coordinamento indipendente per la rete svizzera;
2. **Informer** *"Eos Holding"* : raccoglie informazioni circa lo stato dei mercati europei e le invia ad Etrans;
3. **Executor** *"Atel"* si occupa del commercio di energia e servizi energetici.

Propagazione della vulnerabilità a livello **IPK** nella comunicazione tra il gestore di rete svizzero Etrans e il gestore di rete italiano Grtn



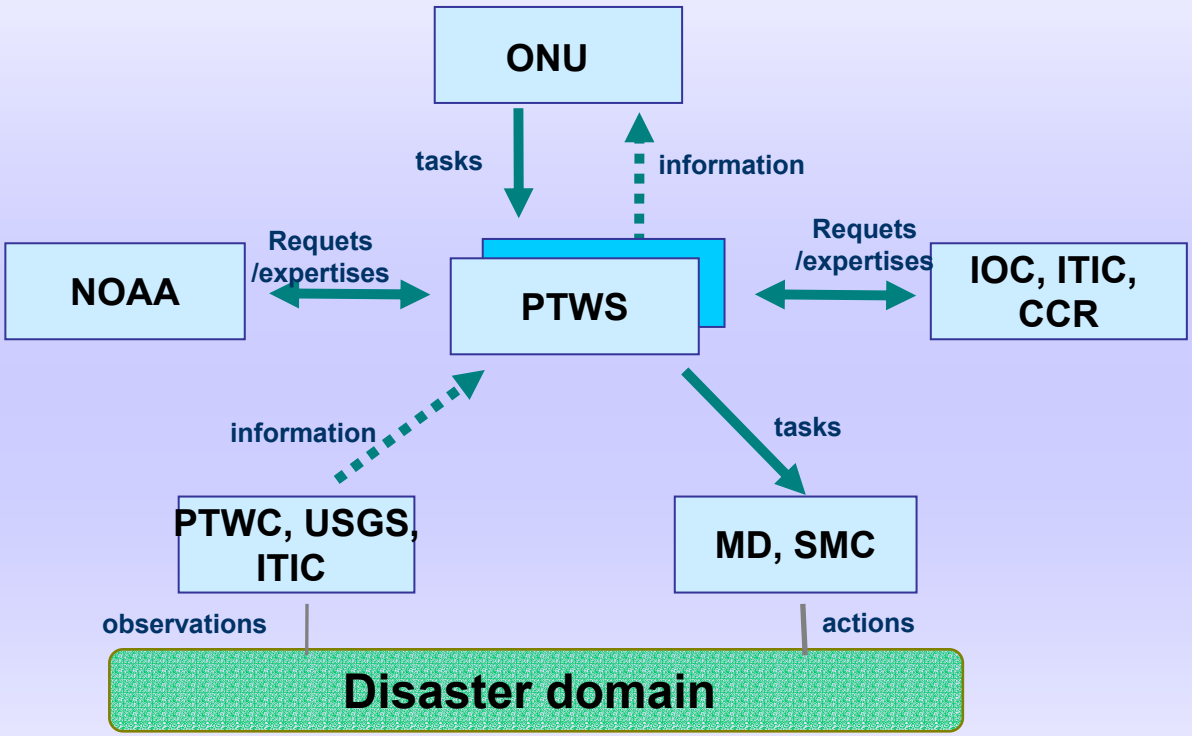
Etrans *(manager svizzero)*

1. *Livello delle informazioni:* l'informazione circa l'interruzione della linea del Lucomanno non viene comunicata tempestivamente al gestore italiano;
2. *Livello delle preferenze:* si sceglie di diminuire il flusso di energia chiedendo al gestore italiano di diminuire la potenza di carico sulla linea;
3. *Livello delle conoscenze*: eccessiva sicurezza nelle proprie competenze e capacità, le procedure standard non vengono attivate.

Grtn *(informer italiano)*

1. *Livello delle informazioni:* le informazioni che vengono trasmesse al gestore italiano sono insufficienti e non utili alla comprensione della situazione di emergenza;
2. *Livello delle preferenze:* le informazioni che vengono trasmesse al gestore italiano sono insufficienti e non utili a stabilire una relazione di preferenza nell'attuale stato di emergenza.

2. TSUNAMI



1. Supervisor *"Onu"* : la sua supervisione si realizza mediante lo IOC;

2. Manager *"Ptws" :* coordinatore dell'attività dei centri operativi;

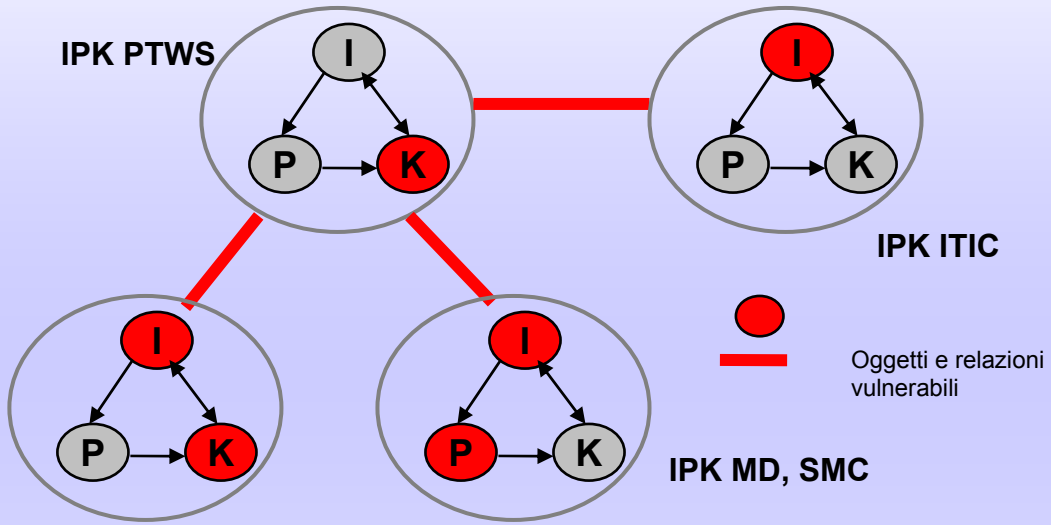
3. Advisor *"Noaa" :* centro specializzato che si occupa della rilevazione degli tsunami nell'Oceano Pacifico;

4. Cooperating manager *"Ioc, Itic, Ccr"* : centri di monitoraggio che assistono il Ptws nella fase di coordinamento delle attività;

5. Informer *"Ptwc, Usgs, Itic" :* si occupa di informare i paesi e le popolazioni che affacciano sull'Oceano Pacifico, sul rischio tsunami

6. Executor *"Md, Smc" :* dipartimenti locali responsabili della gestione dell'allarme.

Propagazione della vulnerabilità a livello IPK nella comunicazione dell'allarme tsunami



Ptws *(manager)* a *livello di consoscenze* non riesce a coordinare le competenze e le attività dei centri meteorologici che gestisce e controlla;

Cooperating manager *(Itic)* a *livello di informazioni* dopo aver registrato le prime scosse non lo comunica allo Ioc che avrebbe potuto contattare i dip. di Stato americano;

Informer*(Ptwc, Usgs, Itic)*

- *Livello delle informazioni:* le 3 stazioni di monitoraggio dopo aver registrato il terremoto non si sono consultate, non c'è stato uno scambio di informazioni;

- *Livello della conoscenza: Usgs* ha comunicato i dati in suo possesso al dipartimento di stato americano perché non ha competenza in materia di maremoti;

Executor *(Md, Smc):*

-*Livello delle informazioni:*Thailandia ed Indonesia hanno perso i contatti con il gruppo ICG, non ricevevano dati ed informazioni aggiornate dal Ptwc;

-*Livello delle preferenze:* le informazioni sono contraddittorie, l'Smc non riesce a stabilire una relazione di preferenza tra i danni causati da un "*probabile*" maremoto e quelli causati da una "*sicura*" fuga disordinata di masse terrorizzate

RISULTATI

TABELLA di Identificazione della vulnerabilità a livello IPK secondo i ruoli UMP nei grandi disastri naturali e nelle infrastrutture critiche

Ruoli / Casi	*Supervisor*	*Manager*	*Cooperating Manager*	*Advisor*	*Informer*	*Executor*
Blackout it.						
Chernobyl						
Linate						
Katrina						
Tsunami						

Legenda:

Il problema si è verificato sul livello delle Informazioni

Il problema si è verificato sul livello delle Preferenze

Il problema si è verificato sul livello delle Conoscenze

Nessun valore dominante

RISULTATI

TABELLA di sintesi qualitativa delle cause che hanno prodotto perdite durante la fase di gestione dell'emergenza o nel corso dell'incidente/disastro.

Cause: / Casi	*Naturale*	*Tecnologico*	*IPK di managers*	*Strutture Organizzative*	*Comunicazione Interna*	*Comunicazione tra organizzazioni*
Blackout it.	*0*	*1*		*1*	*1*	*1*
Chernobyl		*1*	*1*	*1*		*1*
Linate		*1*	*1*		*1*	*1*
Katrina	*0*		*1*		*1*	*1*
Tsunami	*0*		*1*		*1*	*1*

Legenda:

0 – Non evitabili

1 – Evitabili

Non essenziale per lo scenario della Risposta

Essenziale per lo scenario della Risposta

Le interviste

Rappresentazione qualitativa conclusiva delle interviste

Ipotesi / *Interviste*	*Prima Ipotesi*	*Seconda Ipotesi*	*Terza Ipotesi*	*Ottica di interpretazione*
Balducelli	⬆	■ ■ ■	△ ▲ ▲	● ●
Bologna	➡	■ ■ ■	△ ▲ ▲	● ●
Dipoppa	⬇	■ ■	△ ▲	●
Rosato	⬆	■ ■	△ ▲ ▲	● ●
Vicoli	⬇	■ ■	▲ ▲	●

Legenda:

Prima ipotesi: priorità prospettiva socio-cognitiva

Alta ⬆
Medio ➡
Bassa ⬇

Seconda ipotesi: collaborazioni e progetti

Mondiali ■
Internazionali ■
Nazionali ■

Terza ipotesi: cause di vulnerabilità

Tecnologia ▲
Uomo ▲
Organizzazione △

Ottica di Interpretazione:

Fisica ●
Ingegneria ●
Organizzazione ●

Dicono che……

Spesso l'errore risiede nella mancata integrazione fra l'aspetto umano e l'aspetto tecnologico, (…) le reti tecnologiche sono sempre più interconnesse con le reti organizzative. Quando qualcosa si guasta non si riesce sempre a capire se è dovuto ad una limitazione della rete tecnologica o ad una limitazione della rete umana (…) in molti casi c'è anche un concorso di colpa, è molto importante studiare le relazioni, le interrelazioni ed interdipendenze che ci sono tra le reti tecnologiche e le reti umane (Balducelli)

E' possibile trattare contestualmente o comunque con le stesse metodologie sistemi anche molto diversi tra loro, come le infrastrutture critiche, reti di telecomunicazioni e reti sociali. Esattamente come si valutano le vulnerabilità dei sistemi tecnologici, si possono valutare quasi con gli stessi metodi le vulnerabilità dei sistemi umani. (Rosato)

Le infrastrutture organizzative e tecnologiche hanno delle loro vulnerabilità, delle caratteristiche specifiche, che non sono accomunabili, entrambe sono assolutamente importanti ma vanno affrontate con metodi e con strumenti diversi. (Bologna)

Conclusioni

I modelli di vulnerabilità dell'organizzazione che sono emersi con l'applicazione di TOGA includono processi di sviluppo e comportamento di un'organizzazione in stato "patologico" e dovrebbero essere in grado di soddisfare le condizioni di computazionabilità, cioè consentire una futura implementazione nel linguaggio del calcolatore per sperimentazioni di simulazione di tipo "*what-if*".

IPOTESI :utilizzare l'architettura IPK e il paradigma UMP per simulare le patologie e le vulnerabilità dell'organizzazione.

Non è stata presa in considerazione la "*componente emotiva*" che poteva essere legata soprattutto con le preferenze o avrebbe potuto influenzare l'uso delle conoscenze.

Il prossimo passo?? Entrare nei dettagli del problema, considerare all'interno di una possibile simulazione anche questa variabile "emotiva".

E il prossimo passo?……..

Continuare a fare ricerca