La protezione delle Infrastrutture Critiche e il controllo del territorio

Infrastrutture critiche sono *asset* strategici per una nazione: forniscono servizi primari per i cittadini e per il sistema economico e industriale. La loro integrità è necessaria per garantire il livello dei servizi e, spesso, anche la salvaguardia stessa dei cittadini

DOI 10.12910/EAI2017-008

di **Claudio Moriconi**, **Maurizio Pollino** *e* **Vittorio Rosato**, *ENEA*

Le Infrastrutture Critiche (CI *Critical Infrastructures*) vale a dire le reti tecnologiche e per il trasporto di prodotti energetici, arterie per le comunicazioni stradali e ferroviarie, aeroporti e vie per la mobilità e il trasporto delle merci ecc., insieme con altri *asset* strategici (impianti di produzione di energia, stabilimenti di produzione di materiali pericolosi ecc.) definiscono un insieme di risorse verso le quali indirizzare azioni volte a salvaguardare la loro integrità, in modo che riescano a fornire con continuità ed efficienza i servizi e i prodotti necessari ai cittadini e al Paese stesso.
La protezione di tali sistemi deve necessariamente essere *all hazards* (i.e. indirizzata a contrastare tutti i potenziali pericoli che li minacciano) e riguardare sia la loro integrità "fisica" (distruzioni o danneggiamenti da eventi naturali o anche a seguito di attentati ecc.) che quella "cyber", vale a dire la perdita di controllo di tali sistemi. La gran parte di tali sistemi può, e in alcuni casi deve, essere controllata da remoto. La perdita di controllo di tali sistemi è equivalente alla loro distruzione in quanto non consente più agli operatori di potere operare su di essi.
I problemi che rendono complessa la protezione delle CI sono da un lato la complessità intrinseca di tali sistemi tecnologici e, dall'altro, la loro inter-dipendenza funzionale. Le CI si forniscono reciprocamente servizi: il danneggiamento e la conseguente perdita del servizio erogato da uno di essi si ripercuote inevitabilmente (con tempi di latenza più o meno ampi) sugli altri. In questo senso la risposta alla "protezione" di questi sistemi non può che essere olistica, nel senso che deve abbracciare allo stesso tempo tutte le infrastrutture di tale "sistema di sistemi".
Quelle derivanti da danni prodotti da eventi naturali rappresentano una frazione largamente maggioritaria tra tutte le situazioni di mancanza di servizio, ivi comprese quelle prodotte da azioni volontarie dell'uomo. È quindi verso gli eventi naturali che si concentra la maggiore attenzione per

lo sviluppo di sistemi per la protezione delle CI, in grado di predire eventi, di comprendere in quale modo tali eventi possano impattare sugli *asset* e sui servizi, di identificare e quantificare le possibili conseguenze indotte dalle perdite di servizi attese.

Tutto questo assume una rilevanza ancora più marcata allorché si identifichi, nei cambiamenti climatici in corso e nella loro rapida evoluzione, sorgenti di pericolo, in via di aumento in frequenza e intensità[1].

In questa situazione urgono sistemi efficaci che, attraverso una maggiore consapevolezza (*awareness*) del rischio e nella sua predizione, consentano alla Pubblica Amministrazione e agli Operatori delle CI e degli *asset* di mettere in piedi efficaci misure per proteggere e migliorare la Resilienza dei propri sistemi.

La Resilienza ha assunto un ruolo di rilievo in questo contesto: lì dove sia impossibile (a causa dell'intensità di certe manifestazioni naturali) proteggere gli *asset* oltre un certo limite, la *Resilienza*[2] si appresta a diventare *la* proprietà di rilievo per un "sistema di sistemi" come quello delle CI.

La Resilienza è una proprietà che considera la dinamica degli eventi: essa assume un valore globale perché considera i possibili effetti prodotti dalle varie infrastrutture nella loro interazione, la possibilità di azione nelle varie fasi della crisi (dal pre-crisi al post-crisi), indicando una proprietà adattiva del sistema di rispondere ad una situazione di crisi, anche nel contesto di una più articolata visione di "sistema dei sistemi".

La caratteristica vincente del concetto di Resilienza è la sua stessa definizione nei termini della risposta globale del sistema alla perturbazione, considerando tutte le possibili azioni messe in opera prima dell'evento, durante l'evento e dopo l'evento, nella fase di *recovery* e di ripristino delle funzionalità. Pertanto, un'analisi ed una valutazione costante e affidabile dello stato dell'*asset* e una accurata previsione degli eventi sono sicuramente azioni che vanno nella direzione di consentire un aumento della Resilienza.

Protezione delle Infrastrutture: previsione e analisi del rischio

Nel quadro di riferimento tecnico-scientifico precedentemente delineato, il monitoraggio e la protezione delle CI, con particolare riguardo agli aspetti legati alla valutazione del rischio, richiedono l'individuazione di soluzioni in grado di affrontare organicamente le molteplici esigenze e problematiche di tipo tecnologico, ambientale, sociale ecc..

A tal fine, i processi decisionali (in capo a vari soggetti, quali gli operatori/gestori di CI, gli organi di Protezione Civile ecc.) devono poter gestire ed esaminare le situazioni di vulnerabilità e di rischio e, conseguentemente, definire operazioni/strategie da attuare per rispondere a determinate esigenze.

In particolare, in una complessa area metropolitana, dove fondamentale è la tutela dei cittadini e dei beni, i processi decisionali in situazioni critiche dipendono dalla disponibilità e dall'analisi di un ampio set di informazioni, relative alla sicurezza del territorio, al funzionamento delle CI che forniscono servizi primari (i sistemi elettrici e di comunicazione ad esempio) e di emergenza (disponibilità ed efficienza degli ospedali ecc.). In simili contesti, le strategie di valutazione del rischio e gli approcci alla mitigazione di impatti non possono essere affrontati sulla base di un approccio "linearizzato" (vale a dire dove ogni singolo settore venga considerato e analizzato indipendentemente dagli altri): molte e diverse sono, infatti, le dipendenze e le interdipendenze tra i vari settori (un guasto su un settore potrebbe riverberarsi su molti altri, fornendo così *feedback* negativi e quindi un'ulteriore amplificazione degli effetti).

Un approccio globale, come affermato in precedenza, consente di rafforzare la Resilienza, grazie alla previsione di eventi perturbativi (come, ad esempio, quelli di origine naturale) ed alla possibilità di far leva su un ampio insieme di informazioni provenienti dai diversi settori (società, infrastrutture, servizi primari, ambiente ecc.). In questo contesto si inserisce CIPCast, il Sistema di Supporto alle Decisioni (DSS) spaziale, che consente – oltre all'elaborazione in tempo reale di scenari di rischio sulle CI per eventi naturali attesi – anche la simulazione di scenari perturbativi sintetici (terremoti, alluvioni, frane). CIPCast mette a disposizione degli operatori di CI un ampio Database di informazioni, che consentono di:

- migliorare la conoscenza e la comprensione del territorio;
- prevedere scenari esterni, utilizzando sia dati dal campo (sensori) sia le previsioni disponibili;
- stimare i danni attesi sugli elementi delle CI, prodotti da eventi naturali;
- ricavare dalla stima dei danni un'indicazione sulla indisponibili-

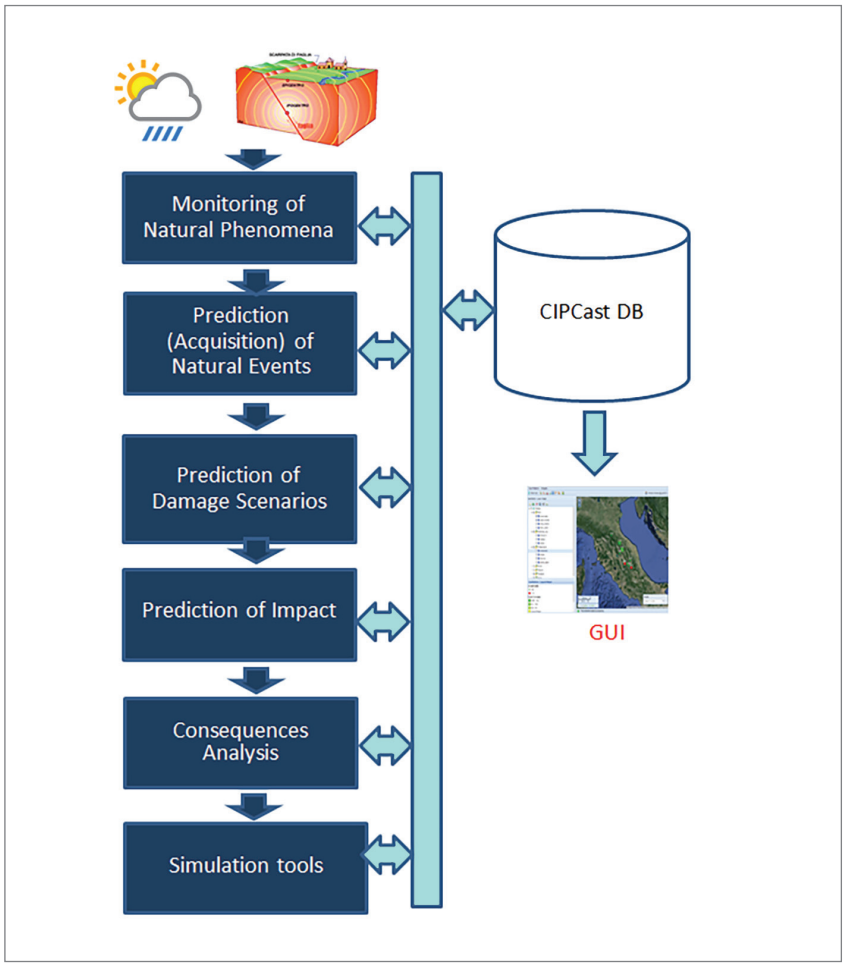

Fig. 1 CIPCast Workflow

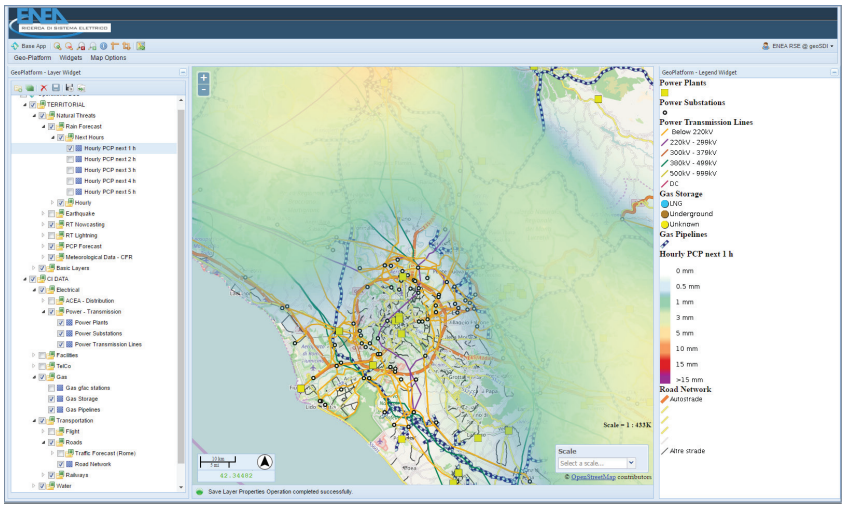

Fig. 2 Interfaccia di CIPCast: visualizzazione interattiva del dato di previsione delle precipitazioni piovose. Il dato di precipitazione (in mm·h-1) è sovrapposto ai layer geospaziali delle CI presenti nell'area di interesse

tà dei servizi erogati, tenendo conto di effetti a cascata e diffusione delle perturbazioni;
- stimare le conseguenze nei riguardi della popolazione e verso altri settori della società;
- supportare la definizione di strategie di ottimizzazione per il ripristino delle infrastrutture.

Su tali basi, CIPCast è stato concepito e progettato come un sistema di tipo *web-based*, in grado di offrire all'utente un'interfaccia geografica *user-friendly* per effettuare analisi spaziali e valutazioni di vulnerabilità e rischio sulle CI d'interesse.

Alla base del *workflow* di CIPCast (Figura 1) vi è la capacità di stimare una serie di fattori di rischio e di potenziale danno, che il verificarsi di un dato evento (inondazioni, precipitazioni piovose intense, terremoti ecc.) potrebbe causare nei sistemi tecnologici. Il Database di CIPCast integra dati di previsione (meteo, *nowcasting*), eventi simici, localizzazione delle frane, dati dai sensori dal campo (stazioni meteo, idrometri ecc.). Il sistema può sfruttare diverse tipologie di dati: Territoriali e Ambientali (cartografia, dati idrogeologici, morfologia ecc.), socio-economici (dati censuari ISTAT), dati infrastrutture tecnologiche, mappe pericolosità/rischio (inventario fenomeni franosi, rischio alluvioni ecc.).

Quindi, effettuata una stima accurata del rischio, il sistema è chiamato a supportare gli operatori di CI ed i gestori dell'emergenza, fornendo informazioni specifiche sullo scenario atteso.

Seguendo l'approccio descritto, il workflow di CIPCast consente di: i) valutare operativamente (24/7) lo stato di rischio degli elementi delle CI in una determinata zona, per minacce legate ad eventi naturali estremi; ii) valutare impatti ed eventuali effetti a cascata, causati da interdipendenze tra i sistemi tecnologici monitorati; iii) supportare gli operatori di Protezione Civile e/o i gestori di CI nelle varie fasi operative (monitoraggio, previsione del rischio, analisi delle conseguenze; oppure per simulazioni, stress test ecc.).

L'interfaccia di CIPCast (di tipo WebGIS) è stata realizzata con l'obiettivo di consentire agli utenti finali di visualizzare gli elementi delle CI e le mappe di rischio, effettuare le analisi sopra descritte, elaborare scenari (Figura 2).

Protezione delle Infrastrutture: ispezione e analisi di infrastrutture complesse

La sorveglianza del territorio costituisce la seconda faccia del controllo delle CI strettamente integrata con l'analisi e la modellazione dei dati che le diverse sorgenti d'informazione di cui l'infrastruttura deve essere dotata forniscono.

Insieme, la sorveglianza e l'analisi dei dati, offrono un ombrello di copertura efficace tanto nei confronti di agenti antropici quanto nei confronti di eventi causati da calamità naturali attivando sia nel primo che nel secondo caso procedure di contrasto rispetto all'evento esterno. Questo ombrello è quello che viene chiamato Resilienza e agisce tanto su eventi con scala temporale molto rapida (come un attacco terroristico) quanto su eventi che

Fig. 3 Paratoie del Mose parzialmente sollevate

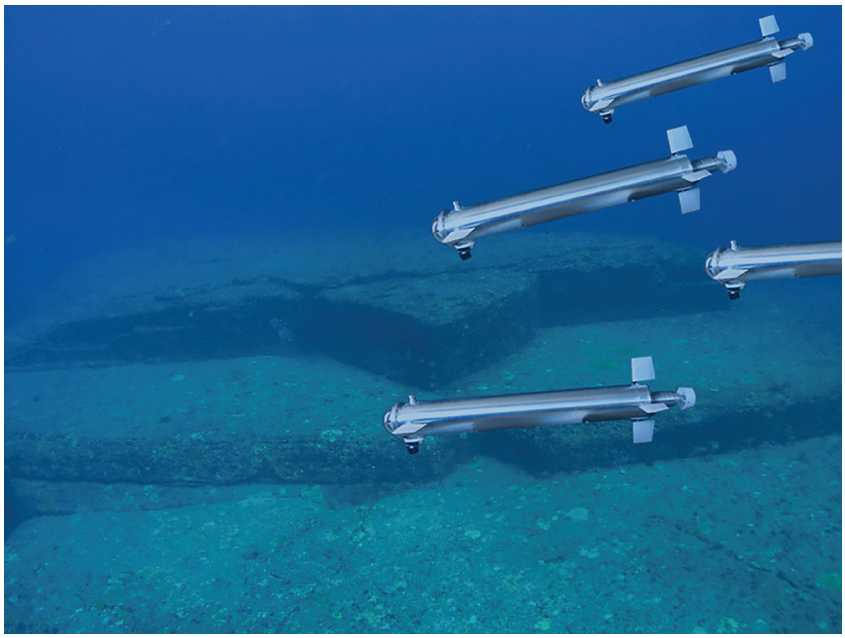

Fig. 4 Robot VENUS – ENEA, avvio di una campagna di test

minacciano l'integrità della struttura su tempi molto più lunghi (come l'erosione legata a fenomeni meteo o di inquinamento) fornendo indicazioni sulla tipologia di danno attesa e sulle modifiche da attuare non solo in termini di contrasto diretto, ma anche di modifica dell'ingegneria dell'opera stessa.

Un esempio che integra entrambe le scale temporali è legato agli accordi in corso di consolidamento tra l'ENEA e il Consorzio Venezia Nuova che sta curando il completamento e la messa in opera dell'infrastruttura MOSE, destinata alla protezione della laguna di Venezia, patrimonio dell'Umanità, e di Venezia stessa dalle modifiche climatiche che stanno moltiplicando la frequenza e l'intensità del ben noto fenomeno dell'acqua alta.

L'opera è costituita da quasi due km di paratoie sollevabili che chiudono tre bocche di porto (di cui una doppia) che separano la laguna dal mare aperto (Figura 3). Si tratta di un opera estremamente complessa, con centinaia di km di tubature sotto pressione, sale di controllo e infrastrutture di cemento e metallo che dovranno resistere all'azione meccanica e di attacco chimico fisico ed anche biologico (es: proliferazione del *fouling*) del mare per decine e forse centinaia di anni e che sono posizionate a profondità che variano tra i sei e i dodici metri.

Un alto livello di Resilienza di una tale infrastruttura è quindi una proprietà estremamente difficile da conseguire e si basa non solamente su un'ingegneria di alto livello, ma anche su altri due elementi critici: la possibilità di un controllo frequente di strutture sommerse e l'integrazione dei dati che da questo controllo provengono in un modello previsionale. Questo modello consentirà la pianificazione dei necessari interventi di mantenimento prima che si verifichino degradi tali da rendere le correzioni più costose e più pesanti per l'operatività dell'infrastruttura stessa. Poiché il controllo tramite squadre di sommozzatori professionisti presenta non solamente costi estremamente elevati, ma anche rischi per la vita umana, il Consorzio Venezia Nuova e l'ENEA hanno concordato di puntare su uno sviluppo tecnologico molto avanzato che consente l'impiego di robot a sciame (sviluppati nei laboratori dell'ENEA e che sono stati riconosciuti come un'eccellenza a livello internazionale, vedi Figura 4) in grado di auto coordinarsi, effettuare riprese delle strutture, sviluppare un'analisi anche dinamica della qualità delle acque e del diffondersi degli inquinanti e soprattutto di comunicare sui fondali ad alta velocità (cosa impossibile allo stato dell'arte) e di ritrasmettere le informazioni raccolte in tempo reale verso la sala di controllo ed il sistema centralizzato di gestione dei dati. La tecnologia, che è attualmente in fase di dimostrazione (la data dell'evento dimostrativo è stata programmata entro il 2017), sarà sviluppata successivamente secondo un programma che prevede oltre al rilascio, nell'arco di un paio di anni, di un sistema di robot telecontrollati operativo, anche un continuo sviluppo tecnologico per far fronte sia alle possibili modifiche delle sfide ambientali, sia alla possibilità di ricadute economiche della tecnologia sviluppata in altre situazioni d'uso. Questo concetto di sviluppo continuo dell'ombrello metodologico e tecnologico di protezione dell'infrastruttura rappresenta il più significativo esempio di Resilienza secondo il profilo descritto in precedenza: non solamente una proprietà intrinseca dell'opera ingegneristica, ma una proprietà dell'intera struttura di *maintenance*, che diventa parte dell'infrastruttura stessa non meno del metallo e del cemento.

[1] Intesa come la capacità di un sistema, o di un gruppo di sistemi dipendenti, di ripristinare rapidamente ed in maniera efficiente il proprio livello di servizio dopo essere stata sottoposta ad una perturbazione di qualche tipo https://www.epa.gov/climate-change-science/understanding-link-between-climate-change-and-extreme-weather

[2] https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Resilience