

## **Topologie, gerarchie e complessità nelle architetture di sistema di *Emergency Operation Center* e di Centrali *Critical Infrastructure Protection*: il ruolo della 3D-COP**

Andrea Fiduccia (\*), Roberto Di Pace (\*\*)

(\*), Intergraph Italia LLC, Via Sante Bargellini 4, 00157 Roma  
Tel. +39.06.43588889; Fax: +39 06 43254376; andrea.fiduccia@intergraph.com

(\*\*) Intergraph Italia LLC, Via Sante Bargellini 4, 00157 Roma  
Tel. +39.06.43588889; Fax: +39 06 43254376; roberto.dipace@intergraph.com

### **Sommario**

Un EOC è un Centro di Comando e Controllo per la gestione di crisi finalizzato a: raccolta, analisi e redistribuzione di informazioni; comando, controllo e coordinamento interagenzia delle operazioni; predisposizione ed attivazione di piani di risposta agli scenari. Per poter svolgere questi compiti un EOC dispone di sistemi di telecomunicazione, di sistemi di *Information Fusion/Common Operational Picture*, di sistemi di intelligence e di sistemi di *calltaking/dispatching*.

Il requisito più critico per un EOC è quello dell'interoperabilità tra i diversi enti coinvolti nella gestione di una crisi. Ogni ente ha, infatti, i suoi sistemi tecnologici (con i relativi formati dati) e le sue specifiche procedure operative. Quindi il problema è sia tecnologico che organizzativo.

L'interoperabilità, visto che le sorgenti di dati sono eterogenee – militari e civili – si ottiene mediante standard condivisi. Nel caso specifico dei dati geografici, lo standard sono i *web service* OGC (WMS, WFS, WCS, ecc.). Di conseguenza, la “Mappa Collaborativa” diviene basata su una *SOA (Service Oriented Architecture)*, cioè uno “*smart client*” (come nella soluzione software Intergraph per EOC europei *I/PR Planning and Response For Emergency Operation Center*).

L'interoperabilità basata su *SOA* comporta però un problema: per poter attingere ai servizi *web* geografici dei provider di dati pubblici civili in una siffatta architettura, l'EOC diviene un nodo di una *Spatial Data Infrastructure*. Quindi l'EOC è ‘aperto’ verso internet e potenzialmente soggetto ad attacchi cibernetici.

Una Sala Operativa CIP – che, invece, monitorizza la sicurezza di una infrastruttura tecnologica - è collegata alla Sala Controllo Impianti Tecnici e deve anche poter gestire eventi di origine naturale. In un sistema CIP vi è una consistente componente di *sensor fusion* (sensori perimetrali e anti-intrusione, videosorveglianza, ma anche monitoraggio parametri di impianto, ecc). Gli allarmi sono per lo più generati dai sensori. Vi è reazione agli eventi (quindi *dispatching*), ma anche pianificazione e scenari. Vi è un *Mobile Resource Management* (le squadre di sicurezza) che coesiste con un *Mobile Workforce Management* (le squadre di manutenzione). Anche in una Sala Operativa CIP i dati geografici ed i flussi di dati dei sensori sono condivisi mediante un'architettura *SOA*.

Un ulteriore livello di complessità, comune alle due classi di sistemi, è dato dal fatto che le Sale Controllo (EOC o CIP) operano secondo logiche di competenza territoriale e secondo gerarchie e topologie.

La *Common Operational Picture 2D/3D* è lo strumento con logica geografica attraverso il quale gli operatori delle centrali interagiscono e collaborano.

Nel paper sono esaminati i requirement funzionali e prestazionali della COP 3D per EOC e CIP con esempi relativi a scenari operativi reali ed alle tecnologie della Intergraph Corporation.

## **Abstract**

An emergency operations center (EOC) is a place where emergency personnel conduct a coordinated response to severe, major events. It typically consists of large building or room reinforced for maximum disaster protection. The building is self-sufficient and can operate for extended periods of time independent of outside power supplies or communications facilities.

It typically performs the following functions: information collection, information processing, information display, information dissemination, management and coordination of interagency activities, implementation of relevant plans, and command and control of assigned resources. Generally, an EOC includes communications links (i.e. telephones, two-way radios, patching equipment); computer equipment; map displays to show geographic attributes; dynamic data of the unfolding situation; static reference data; and response plans. This paper presents typical EOC requirements, and the technology available to address them.

EOCs need technology and tools that provide them with real-time collaboration, external data fusion, situational awareness, financial tracking, status reporting, and resource and consequence management.

Any EOC solution must meet specific standards. EOCs must report using a standard format and meet basic government policy and requirements for regulations (i.e. U.S. standards such as the National Incident Management System NIMS and international standards such as the Association of Public Safety Communications APCO). Another interoperability framework is based on SOA Service Oriented Architecture and particularly it is built using OGC's web services (WMS, WFS, WxS, etc).

Protecting critical, geographically dispersed infrastructure represents an enormous challenge. Damage to power plants, roads, and other critical infrastructures could cause severe human and economic loss.

Effective solutions for Critical Infrastructures Protection provide decision makers a common operating picture for all locations and resources, at all times throughout a security event, while maximizing the use of all available information, technologies, and manpower.

The goal is to take advantage of available sensors, security technologies, and personnel to provide security in a cost-effective manner. Central to the solution is a command and control system that integrates technologies such as global positioning systems, video, or security sensors on an easy-to-view, map-based interface. This helps regional command centers coordinate and communicate before, during, and after an event. Interoperability of CIP systems is built on SOA and OGC's web services.

Both EOCs and CIPs Control Rooms operate having a geographical area of competency and a hierarchy and a topology in a network structure.

The Common Operational Picture is the main collaborative environment.

The functional and performance requirements for 3D/2D COP are exposed in the paper. The requirements are compared with some case histories.

## **EOC e Protezione Civile**

Per introdurre il concetto di gerarchia e topologia in una rete di EOC ci serviremo di una rappresentazione concettuale dei flussi informativi per un evento di tipo "b".

Ricordiamo che *"in caso di eventi che colpiscono un territorio, il Sindaco ha il compito di provvedere ad assicurare i primi soccorsi alla popolazione, coordinando le strutture operative locali, tra cui i gruppi comunali di volontariato di protezione civile. Se il Comune non riesce a fronteggiare l'emergenza - evento di tipo "a" - su sua richiesta intervengono la Provincia, gli Uffici territoriali di governo, cioè le Prefetture, e la Regione, che attivano le risorse di cui dispongono - evento di tipo "b". Nelle situazioni più gravi, su richiesta del Governo regionale, subentra il livello nazionale, con la dichiarazione dello stato di emergenza - evento di tipo "c". In questo caso il coordinamento dell'intervento viene assunto direttamente dal Presidente del Consiglio dei Ministri, che opera tramite il Dipartimento della Protezione Civile"*.

Rispetto alla tipologia di eventi, il “Metodo” della Protezione Civile prevede un articolato sistema di comando e controllo rappresentato, nelle sue componenti essenziali, in Figura 1.

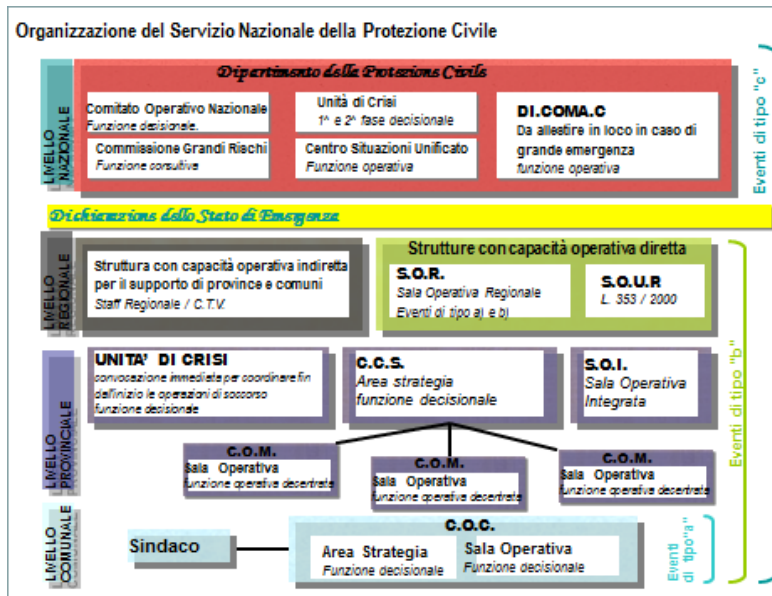


Figura 1 – Elementi principali dell’organizzazione della Protezione Civile (Fonte: VVFF).

Ricordiamo le caratteristiche di alcune delle componenti funzionali ed operative riportate in Figura 1.

- La **DI.COMA.C. (Direzione di Comando e Controllo)** “rappresenta l’organo di coordinamento delle strutture di Protezione Civile a livello nazionale in loco, secondo quanto stabilito da accordi internazionali. Tale organo viene attivato dal Dipartimento della Protezione Civile, in seguito alla Dichiarazione dello Stato di Emergenza. La sede operativa della DI.COMA.C. deve essere ubicata in una struttura pubblica posta in posizione baricentrica rispetto alle zone di intervento”.
- Il **C.C.S. (Centro di Coordinamento Soccorsi)** “rappresenta il massimo organo di coordinamento delle attività di Protezione Civile a livello provinciale. Esso è composto dai responsabili di tutte le strutture operative presenti sul territorio provinciale. I compiti del C.C.S. consistono nell’individuazione delle strategie e delle operatività di intervento necessarie al superamento dell’emergenza attraverso il coordinamento dei Centri Operativi Misti (COM). Nell’ambito dell’attività svolta dal C.C.S. si distinguono una "area strategia", nella quale afferiscono i soggetti preposti a prendere decisioni, ed una "sala operativa" nella quale operano 14 funzioni di supporto dirette da altrettanti responsabili. La sala operativa deve avere una suddivisione interna tale da poter ospitare in ambienti distinti le seguenti funzioni di supporto: -Tecnica e di Pianificazione (molteplici competenze e varie amministrazioni); -Volontariato (numerose organizzazioni che partecipano all’emergenza); -Strutture operative (dei Vigili del Fuoco, delle Forze Armate, delle Forze dell’Ordine); -Telecomunicazioni (Sala radio separata a causa del rumore di fondo); -Mass Media e Informazione (Sala Stampa limitrofa ma al di fuori della sala operativa)”.
- Il **C.O.M. (Centro Operativo Misto)** “è una struttura operativa che coordina i Servizi di Emergenza. L’ubicazione del C.O.M. deve essere baricentrica rispetto ai Comuni afferenti e localizzata in strutture antisismiche, realizzate secondo le normative vigenti, non vulnerabili a

qualsiasi tipo di rischio. Le strutture adibite a sede C.O.M. devono avere una superficie complessiva minima di 500 m2 con una suddivisione interna che preveda almeno: -una sala per le riunioni; -una sala per le Funzioni di Supporto; -una sala per il Volontariato; -una sala per le Telecomunicazioni. Tali strutture devono essere dotate di un piazzale attiguo che abbia dimensioni sufficienti ad accogliere mezzi pesanti e quanto altro occorra in stato di emergenza”.

- Il **C.O.C. (Centro Operativo Comunale)** “è il centro operativo a supporto del Sindaco, autorità di protezione civile, per la direzione ed il coordinamento dei servizi di soccorso e di assistenza alla popolazione. Tale centro dovrà essere ubicato in strutture antisismiche, realizzate secondo le normative vigenti, ed in aree di facile accesso e non vulnerabili a qualsiasi tipo di rischio. Tali strutture devono essere dotate di un piazzale attiguo che abbia dimensioni sufficienti ad accogliere mezzi pesanti e quanto altro occorra in stato di emergenza. Si dovranno individuare nelle grandi città i quartieri o le circoscrizioni, mentre per le altre tipologie insediative le località e le frazioni”.

Adesso analizziamo i flussi dei dati nel caso di un evento di tipo “b” (Figura 2).

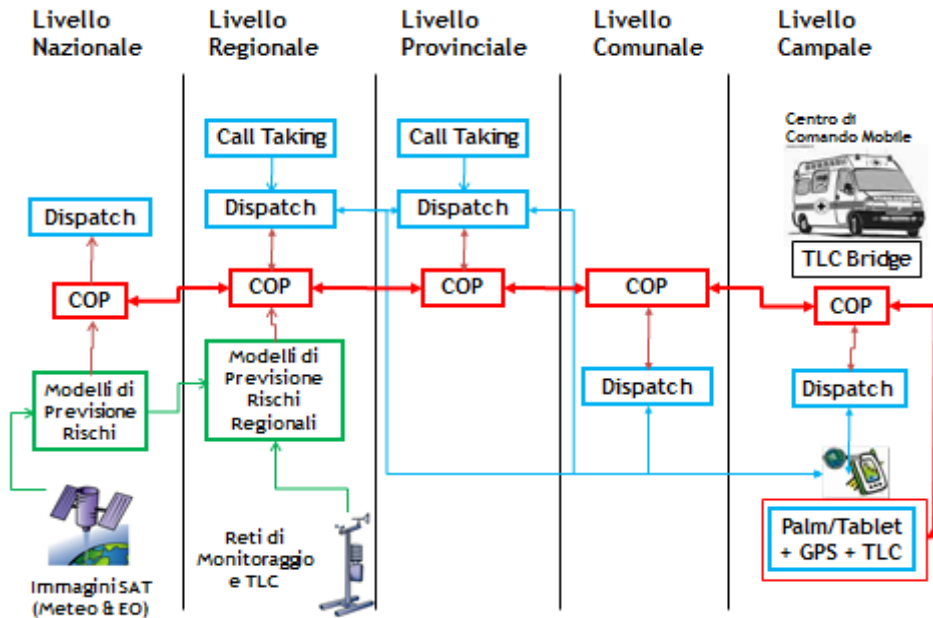


Figura 2 – Flussi di informazioni in un evento di tipo “b”.

I flussi rappresentati in Figura 2 sono classificabili secondo tre tipologie:

- **CallTaking/Dispatching** (elementi in azzurro) – sono i flussi di dati tipici di una sala gestione emergenze; alcuni operatori (*calltaker*) rispondono a chiamate di richiesta soccorso che arrivano mediante chiamate telefoniche dei cittadini e analizzano segnalazioni di eventi critici attivate da allarmi delle reti di monitoraggio, altri operatori (*dispatcher*), sulla base della “validazione” degli eventi operata dai *calltaker*, assegnano le risorse agli eventi e ne seguono l’evoluzione.
- **Common Operational Picture** (elementi in rosso) – è l’ambiente collaborativo basato su tecnologie GIS (2D e 3D) nel quale sono visualizzate le posizioni delle chiamate e degli allarmi

provenienti rispettivamente dal sottosistema di *CallTaking/Dispatching* e dalle reti di monitoraggio, le previsioni dei modelli e le posizioni delle risorse in campo.

- **Modelli e Reti di Monitoraggio** (elementi in verde) – appartengono a questa tipologia flussi di dati di sistemi eterogenei (immagini di satelliti per l'osservazione della terra, immagini di satelliti meteorologici; reti di sensori idropluviometrici, sensori per il monitoraggio delle frane, modelli matematici di previsione meteorologica e di scenari di rischio a partire dai dati dei sensori).

I tre flussi sono diversamente generati e fruiti dai nodi della catena decisionale della Protezione Civile. La necessaria interoperabilità è garantita da standard condivisi.

Una prima standardizzazione è a livello architetturale ed è fondata sulla *SOA - Service Oriented Architecture*, cioè su di un'architettura basata su *web service*.

In particolare, per i dati geografici si adottano i web service OGC (WMS, WFS, WCS, etc).

L'esperienza del progetto *SensorNet*, il sistema net-centrico che integra sensori, servizi e dati per l'*Homeland Security* negli USA, ha dimostrato l'applicabilità dei *web service* OGC anche all'interoperabilità dei flussi di dati dei sensori per il rilevamento intrusioni e per il rilevamento di sostanze pericolose (*CBRNE - Chemical, Biological, Radiological, Nuclear and Explosive*). Per ottenere un'architettura *plug-and-play* è stato sviluppato lo standard IEEE 1451. In *SensorNet* tutte le "entità" sono geografiche e, conseguentemente, la struttura dati di base è realizzata a partire dallo standard OGC WFS (dato geografico vettoriale + dati alfanumerici codificato in GML) coniugato ad un'architettura di sicurezza basata su certificati.

Il prototipo di *SensorNet*, realizzato dall'Oak Ridge National Laboratory (ORNL), Intergraph, ObjectVideo e dal Directorate of Emergency Service di Fort Bragg, è l'Integrated Incident Management Center (I<sup>2</sup>MC) di Fort Bragg. I "dati sensori sono "fusi" – geograficamente – con i dati (video e traiettografia) generati dall'*Intelligent Video Surveillance System (IVSS)* nella *Common Operational Picture* a partire dalla quale il *dispatcher* attiva la gestione dell'evento.

Un altro livello di interoperabilità sono i protocolli, come il *CAP (Common Alerting Protocol)* e il "*Dizionario TSO (Tactical Situation Object)*", per l'interscambio di messaggistica in un contesto di gestione dell'emergenza.

Appare chiaro, a nostro avviso, che i singoli nodi del network decisionale sono, dal punto di vista dei dati geografici, nodi di una *Spatial Data Infrastructure*. A tal proposito è importante sottolineare che l'interoperabilità OGC è di tipo sintattico (cioè relativa al modello fisico del dato comprendente anche il sistema di coordinate geodetico-cartografiche), ma non entra nelle problematiche di tipo semantico. Le codifiche degli attributi e l'organizzazione logica degli strati informativi sono esempi di problemi che appartengono al campo dell'interoperabilità semantica. Se due enti territoriali confinanti, che hanno competenza per la realizzazione dello stesso strato informativo, lo strutturano diversamente da un punto di vista concettuale e logico, ne compromettono l'usabilità.

A livello europeo, la Commissione ha riconosciuto l'importanza della disponibilità dei dati geografici in quantità consistenti ed in modalità di fruizione condivisa e mediante la Direttiva INSPIRE (2007/2/EC) ha posto le basi legali per la European Spatial Data Infrastructure costituita sulle SDI "standardizzate" dei singoli Stati Membri e con una focalizzazione iniziale sulle tematiche ambientali.

INSPIRE ha previsto che, nel periodo 2006-2008, venissero definite le regole per realizzare le Infrastrutture di Dati Territoriali nei vari paesi dell'Unione Europea.

Queste regole sono dette Implementing Rules e sono finalizzate all'interoperabilità dei servizi ed all'armonizzazione delle informazioni geografiche in ambito europeo.

Per favorire il decollo di INSPIRE - e dell'iniziativa ad essa vicina *GMES (Global Monitoring for Environment and Safety)* - la Commissione Europea finanzia, attraverso vari Fondi (FP6, FP7, eContentPlus) progetti pre-operativi. In particolare per lo sviluppo dei Data Models dei dati dell'Annex II la Commissione individua dei *Reference Project* che operano in *clustering* con il JRC.

Ad oggi, la modalità tecnica individuata per la data harmonization è quella del “data remodeling”: a “livello INSPIRE” vengono individuati i *common data model* per le varie tipologie di dati e i *data provider* condividono le loro banche dati trasformandole, a rigore “*real time*”, secondo i *common data model* o come *web service* WMS (o, preferibilmente, WFS) ovvero rendendo il dato scaricabile in GML 3.2.

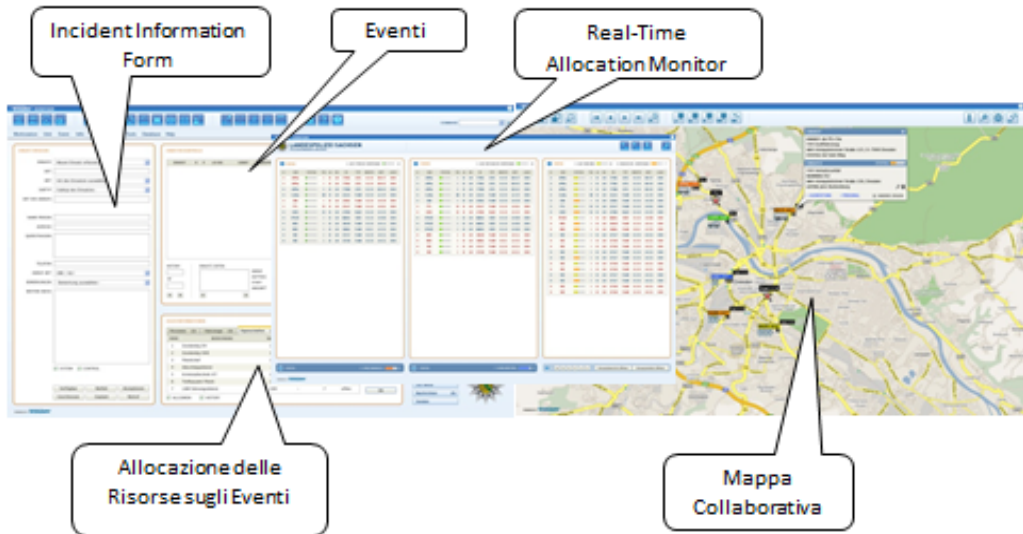


Figura 3 – Common Operational Picture in una Sala Gestione Emergenze (Tecnologia I/CAD - Intergraph Computer-Aided Dispatch).

Da quanto sin qui evidenziato, si possono dedurre i *requirements* per la COP.

1. La COP è un client per *web service* OGC erogati da SDI (e, nell’EU deve essere *compliant* con le “regole tecniche” di INSPIRE)
2. La COP deve poter funzionare in presenza di banda ridotta e in caso di interruzioni della rete, quindi deve disporre di *caching* “intelligente” dei dati (sia lato client che lato server).
3. La COP deve poter interfacciare *data streaming* di sensori e traiettografia di risorse mobili.
4. Deve esistere una “COP leggera” per dispositivi palmari.
5. La COP è una “mappa collaborativa”, quindi implementa strumenti ottimizzati per utenti che non sono specialisti di informazione geografica.
6. La disponibilità della visualizzazione 3D permette di avere un’interfaccia più intuitiva e di disporre di funzionalità a valore aggiunto (intervisibilità, modelli di simulazione, ...).
7. A differenza di un applicativo cartografico da Sala Gestione Emergenze – che è orientato alla gestione del ciclo chiamata-intervento – la COP di un EOC è orientata ad attività che non devono essere necessariamente legate ad una “chiamata”, bensì ad una pianificazione e deve, conseguentemente, implementare specifici strumenti.
8. La COP deve avere un Resource Management System per la gestione di personale e attrezzature.

Dunque, la COP non è un semplice “sistema cartografico” da sala operativa. Non a caso, Intergraph Corporation che detiene una posizione di leadership di mercato nel settore delle Sala Gestione Emergenze (paradigma della Centrale a Numero Unico – “9-1-1” negli USA e “1-1-2” in Europa), ha sviluppato una specifica linea di prodotti per gli EOC anche sfruttando la grande esperienza maturata nel settore delle SDI.



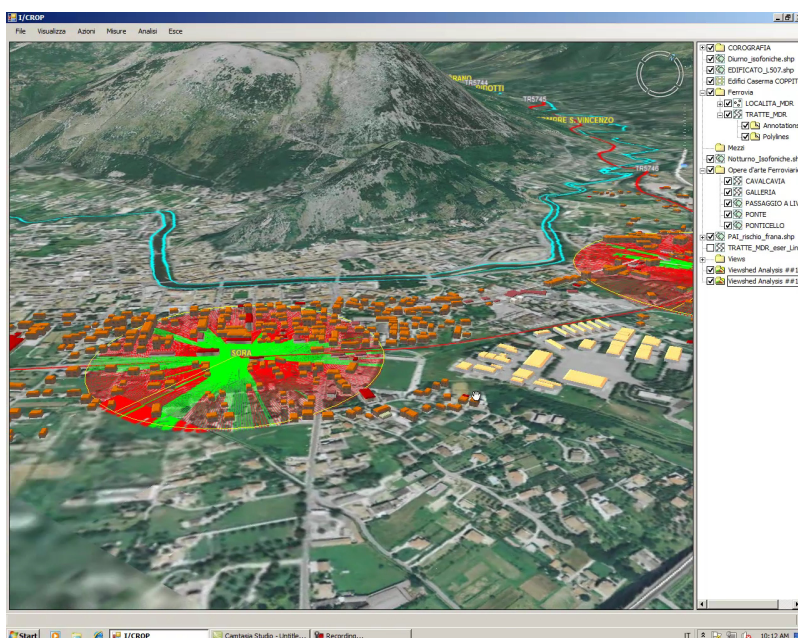


Figura 4 – Common Operational Picture 3D (Tecnologia I/CROP I<sup>2</sup>RMS - Intergraph Incident and Resource Management System).

La Intergraph Corporation, infatti, ha partecipato a progetti collegati ad INSPIRE cofinanziati dalla Commissione Europea quali il progetto HUMBOLDT (GMES Global Monitoring for Environment and Security), i progetti GIS4EU, EURADIN, eSDI-Net+, NATURE-SDIplus (eContentPlus), il progetto CAFÉ (SEIS - Shared Environment Information System) e partecipa al European Security Research Programme (ESS).

Poi, Intergraph ha sviluppato in Europa diversi progetti di SDI a livello nazionale e regionale collegati ad INSPIRE: i GeoPortali della Repubblica Ceca e della Polonia; le SDI delle Asturie (IDEAS) e della Galizia (IDEG) e il Progetto IDERioja in Spagna; la IDT della Regione Veneto in Italia; etc.

Una prima soluzione per gli EOC è un'architettura "ibrida" nella quale le architetture gerarchiche rigidamente client-server proprie delle "centrali 9-1-1" (tecnologia I/CAD - **Intergraph Computer-Aided Dispatch**) sono integrate con sistemi basati su *SmartClient* per il *dispatching* "leggero", per le funzionalità di COP-client SDI e di condivisione di tool di pianificazione in ambiente web (tecnologia I/PR – **Intergraph Planning and Response For Emergency Operation Center**). Questo approccio è stato adottato per il sistema integrato di sale controllo della Polizia della Sassonia (13 sale controllo della polizia con integrazione della rete radio digitale TETRA e sistemi di Coordinamento Interagenzia e di Mappa Collaborativa con data fusion tra i dati di intervento e le sorgenti di informazione geografica istituzionale della *Spatial Data Infrastructure* della Sassonia).

Nella Sala Operativa del G8 a L'Aquila nel 2009, invece, Selex Sistemi Integrati (FinMeccanica), prime contractor incaricato dal Dipartimento Nazionale della Protezione Civile per la gestione dell'evento G8, ha utilizzato per la Common Operational Picture la consolle **Intergraph Geospatial Integrator for Onsite Troops and Tracks Observation**. Tale tecnologia è parte integrante del sistema di pianificazione, monitoraggio e controllo proposto da Intergraph Italia nell'ambito della gestione grandi eventi e gestione emergenze che rende disponibile agli operatori dei vari Enti delle varie Funzioni, interfacce dedicate 2D e 3D, funzionalità avanzate di interrogazione, annotazione e condivisione di informazioni.

**Common Operational Picture 3D e sistemi Critical Infrastructure Protection**

I sistemi *Critical Infrastructure Protection* presentano molti aspetti in comune con gli EOC in quanto devono interfacciare nella COP dati geografici con *streaming* di sensori. In un contesto di sicurezza è routine la pianificazione, situazione eccezionale quella di “evento” e vi è un aspetto duale di *Mobile Resource Management* (sicurezza) e di *Mobile Workforce Management* (manutenzione). Nel segmento di mercato della *Critical Infrastructure Protection*, caratterizzato dalla necessità di interfacciare il sistema di *security* con il sistema di gestione tecnica dell’infrastruttura critica, un ulteriore vantaggio competitivo di Intergraph è dato dal fatto che la divisione **Intergraph PP&M** è il leader di mercato nel segmento dei software per la progettazione e gestione degli impianti industriali e che molte grandi Utilities hanno informatizzato le loro reti con il software **Intergraph G/Technology**.

Nel caso dei sistemi CIP, quindi, ulteriori funzionalità sono richieste alla COP3D:

9. La COP deve integrare la *data fusion* da sistemi radar o da *videanalytics* avanzate.

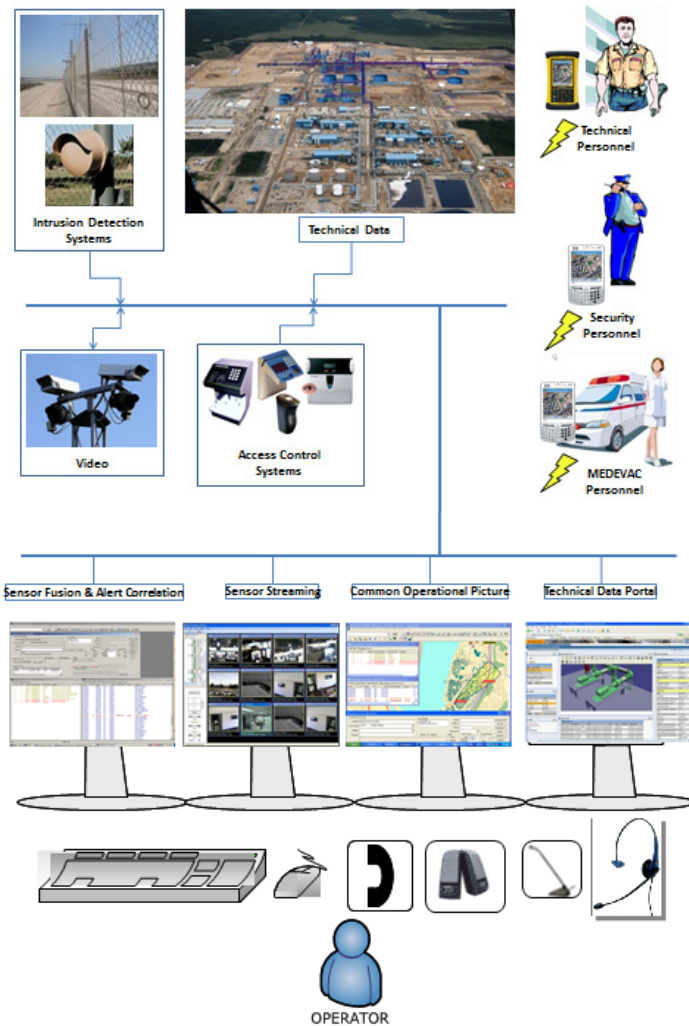


Figura 5 – Sistema Critical Infrastructure Protection Intergraph (I/Security Framework, SmartPlant Enterprise for Owner Operators).



10. La COP deve riportare lo stato dei sensori di controllo perimetrale e, con particolare riferimento alle Camere PTZ, deve essere visibile nella COP il *field of view* coperto dalle singole camere e deve essere possibile selezionare dalla COP lo streaming delle videocamere (che poi verrà visualizzato nell'ambiente di *exploitation*) e pilotare il brandeggio delle videocamere.
11. Nella COP deve essere possibile vedere tridimensionalmente gli impianti tecnici, con possibilità di identificarne gli elementi, accedere ad informazioni sul funzionamento dell'impianto interfacciando lo SCADA e i cosiddetti sistemi PA-GA-SA (*Public Address - General Alarm - Sensor Alarm*) per gli allarmi relativi a malfunzionamenti o emergenze (analisi fumi, anomalie termiche, antincendio, etc).

Tali requisiti sono soddisfatti dalla componente COP 3D della soluzione Intergraph I<sup>2</sup>RMS.

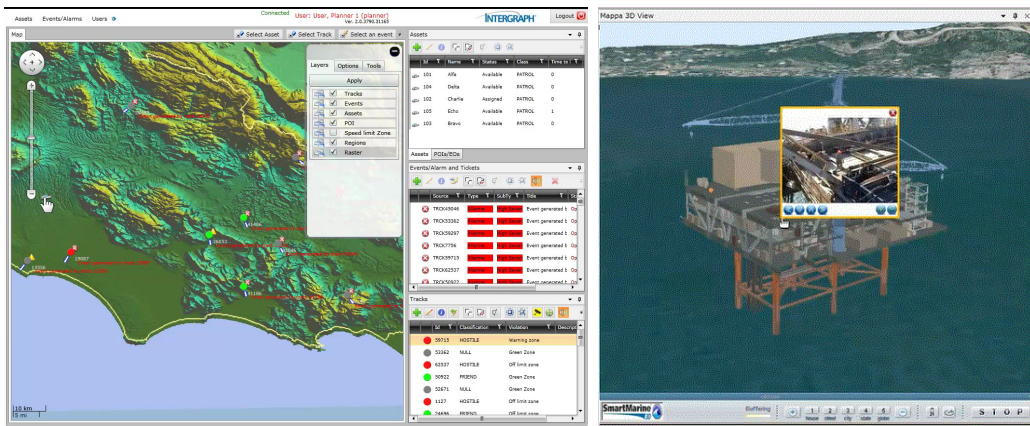


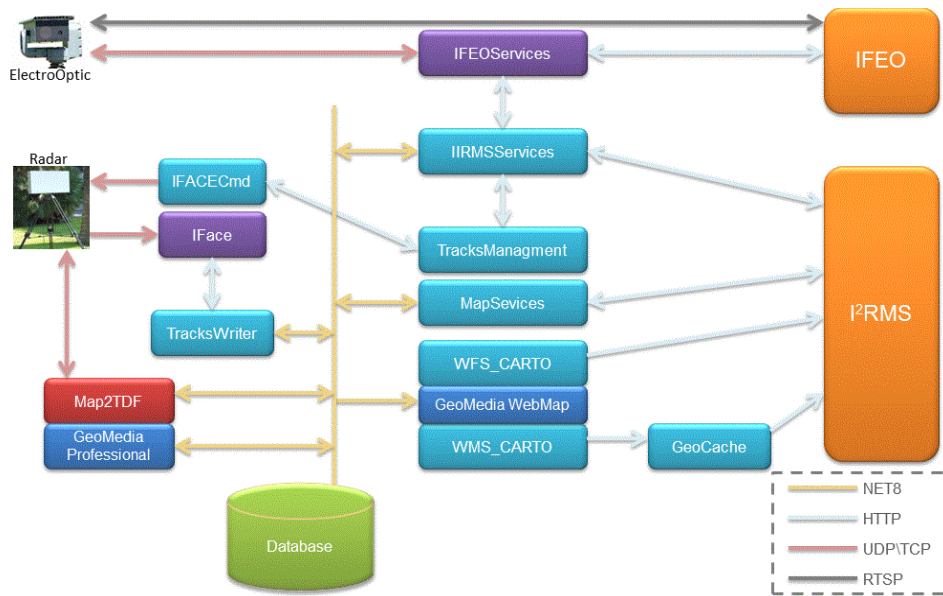
Figura 6 – COP 2D e 3D in I<sup>2</sup>RMS.

Un'altra problematica propria delle soluzioni CIP, e risolta mediante la soluzione I<sup>2</sup>RMS da Intergraph, è quella delle diverse possibili gerarchie/topologie dei network decisionali. In genere, il network decisionale ha una struttura a tre livelli:

- Livello 1. Sito remoto di sensori. Un esempio può essere un sito che ospita un radar di sorveglianza marittima e una camera multispettrale *long range*, con i relativi sistemi di alimentazione e di telecomunicazione. Talvolta questa tipologia di siti è presidiata da personale che può gestire direttamente i sensori oppure si tratta di sistemi pilotati da remoto.
- Livello 2. Centrale di Controllo “Locale” che ha la responsabilità per una certa area territoriale o funzionale comprendendo diversi siti di Livello 1.
- Livello 3. Centrale di Controllo “Primaria” dell'intero sistema che ha, conseguente, la COP dell'intera infrastruttura critica.

A partire da questa struttura si possono ottenere più configurazioni operative - ricordiamo che una caratteristica peculiare di alcune infrastrutture critiche è quella di avere una rilevante estensione territoriale (si pensi ad una infrastruttura di trasporto o di trasmissione dell'energia o ad una *pipeline*).

In un primo scenario, il ruolo operativo principale è svolto dalle Centrali di Controllo di Livello 2. Ad esse è data la missione di gestire le crisi nella loro area di competenza disponendo di forze di reazione autonome, mentre la Centrale di Livello 3 monitorizza la situazione complessiva, ma non dispone di risorse per interventi. Le Centrali di Livello 2 possono telecontrollare i sensori dei Siti di Livello 1. Talvolta la Centrale di Livello 3 dispone di reti di sensori remoti di Livello 1 che gestisce direttamente.



<b>I²RMS</b>	Application for Incident and Resource management	<b>IFACECmd</b>	WS for Radar control
<b>IFE0</b>	Application for Electro-Optic Device control	<b>IFace</b>	Windows Service for UDP listening of trajectories and asset provided by TDF
<b>IFE0Services</b>	Windows Service for connection with RCU library	<b>Map2TDF</b>	Desktop application for design and publishing (to Radar) of Attention Zones
<b>GeoMedia Products</b>	GeoMedia Professional and GeoMedia WebMap	<b>Database</b>	Primary DataBase (GeoDB-enabled)
<b>IIRMServices</b>	WS for access, data management and interfaces of I²RMS		
<b>TracksManagement</b>	WS for radar I/O data flows		
<b>MapSevices</b>	WS for mapping components		
<b>TracksWriter</b>	WS for radar tracks data coming from IFACE		
<b>WFS_CARTO</b>	WS (GeoMedia WebMap) for WFS data publishing		
<b>WMS_CARTO</b>	WS (GeoMedia WebMap) for WMS data publishing		
<b>GeoCache</b>	WMS Cache		



Figura 7 – Intergraph I²RMS: architettura di un singolo “nodo”.

In altri scenari, la Centrale di Livello 1 dispone di sue forze di reazione e può andare in sostituzione (*over-ride*) delle Centrali di Livello 2 laddove dovesse ravvisare un mancato intervento e telecontrollare tutti i Siti di Livello 1.

Tra questi due scenari “estremi” se ne possono situare di ibridi e il network decisionale prevede, poi, siti di mirroring per i repository di informazioni critiche che operano tra loro secondo logiche di *disaster recovery*.

Dunque, ad soluzione tecnologica di Comando e Controllo per sistemi di Protezione di Infrastrutture Critiche è richiesta una grande flessibilità di configurazione. In Figura 7 è rappresentata la struttura di un “Nodo I<sup>2</sup>RMS” ed in Figura 8 un esempio di architettura per sistema CIP su tre livelli.

Ancora una volta la soluzione al problema è nella *Service Oriented Architecture*.

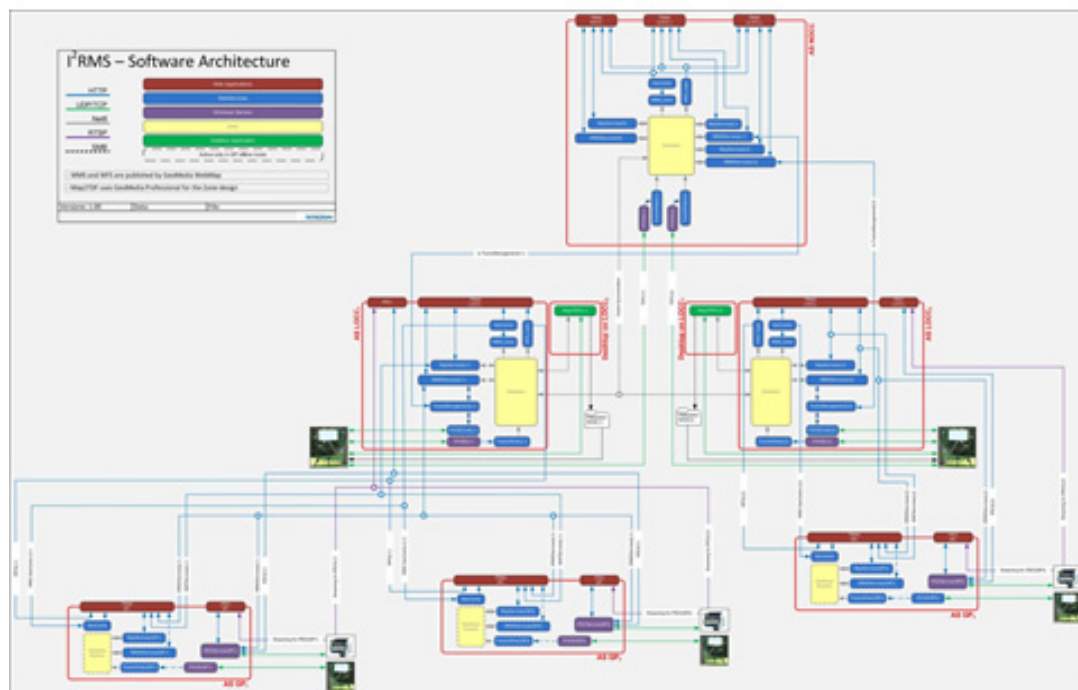


Figura 8 – Intergraph I<sup>2</sup>RMS: esempio di architettura di sistema CIP su tre livelli.

In conclusione, quanto esposto nel presente paper documenta il *commitment* della Intergraph Corporation nel realizzare soluzioni software a standard industriale (*COTS – Commercial-Of-The-Shelf*) nel settore dell'informazione geografica che costituiscono, da oltre 40 anni, un riferimento a livello mondiale, in termini di efficienza ed affidabilità, per le sale operative della pubblica sicurezza, dei vigili del fuoco, per l'emergenza sanitaria, per la Protezione Civile e per la protezione delle infrastrutture critiche. Di fatto, nel mondo, una persona su dodici è “protetta” da sistemi Intergraph.