WHITE PAPER

Critical Infrastructure Protection (CIP)

Solutions for Energy, Utilities, and Communications Companies

INTERGRAPH®

Contents

1. Introduction – The Threat

When disaster strikes, whether it originates naturally or by human hands, destruction can be far-reaching, affecting both the direct-hit location as well as the interwoven systems that support it. Events such as the World Trade Center and Pentagon attacks on September 11, 2001, the London Underground bombings on July 7, 2005, and Japan's most recent earthquake-triggered tsunami on March 11, 2011, have all demonstrated the need for critical infrastructure protection. It is futile to assess what precautionary actions should have been taken after a disaster. Following these calamities, the global perspective has swayed toward addressing preventative measures for vital infrastructures before the next tragedy occurs.

In the United States, the Homeland Security Advisory system was formed under the advice of the Department of Homeland Security (DHS) to secure all government and critical sector levels during crucial moments. *The National Strategy for Physical Protection of Critical Infrastructure and Key Assets* is a DHS document that outlines a collection of national standards for securing key infrastructure and resources essential for functionality within the government, economy, national security, and public sectors.

Similarly, Europe established The European Union Program for Critical Infrastructure Protection (EPCIP) in December 2005 (five months after the London bombings). The EPCIP describes critical infrastructure as "an asset, system, or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic, or social well-being of people, and the disruption or destruction of which would have a significant impact."[1]

The Asia-Pacific region is also following suit, particularly in the oil and gas infrastructure protection market. As a result of terrorist attacks, sabotages, and other various offenses, expanded refineries equipped with security system upgrades are becoming more prevalent. According to Business Wire, "As Asia Pacific is the largest consumer of oil and gas, governments and energy companies have accorded priority to protecting the infrastructure of the oil and gas installations, with some countries even mandating the deployment of security systems."2

For utilities, pipelines, and communications companies, CIP and disaster management are serious concerns. Being able to communicate exactly where facilities and resources are located, as well as dispatching, guiding, and tracking the movement of emergency personnel to a specific location, are fundamental to effective collaboration and response.

Securing critical infrastructure, such as utilities, dams, oil refineries, and government installations, is essential to fighting terrorism and mitigating the effects of other catastrophes. To accomplish this, security planning must anticipate intelligent, adaptive adversaries and large-scale emergencies that create terror and confusion and complicate response by causing multiple, simultaneous incidents. In those circumstances, the sheer volume of inputs from alarms, sensors, closed-circuit televisions, and situational reports can overwhelm a security team and provide a confusing picture of the unfolding situation. That's why security systems must do more than provide raw information – they must provide automation, intelligence, and interoperability to streamline work processes and maximize the protection of people and property. Intergraph's Security Solutions for Critical Infrastructure provide domain awareness in day-to-day operations, as well as emergency incidents, and the ability to execute multi-tiered security plans. Our common operational picture integrates technology, sensors, communications, data, and more – giving you the advantage of real-time, actionable intelligence for energy, utility, and communication networks.

2. Industry Sectors – The Need

2.1 Electric Utility Industry

Electricity is the vanguard for success in nearly all operational facilities, from communal areas, such as schools and hospitals to revenue-generating zones, such as businesses and manufacturing plants. It is also required for generating new forms of energy, like refined oil. If a large-scale or prolonged interruption of power were to take place, it would disable numerous crucial functions of the economy and national defense – paralyzing the pursuit of response and recovery.

Consider a scenario involving an electric-powered infrastructure. After a failure of the electric network at a critical location, other systems soon fail. Sewage pump stations running on standby cease to operate, cash machines fail, and the banking industry soon collapses. Simulations have revealed that economies largely dependent on electronic devices will turn into cash-only economies, providing evidence that CIP for the electric utility industry is a vital and necessary global initiative.

The electrical industry covers significant plots of geography, making it a highly intricate system of assets (i.e., generation facilities, key substations, switchyards, etc.) with its own unique set of protection challenges.

Supplying redundancy and increasing generating capacity translates into a dependable electricity service, according to some transmission or distribution facilities. This method, unfortunately, is wrought with many issues that may keep owners and operators of electrical facilities from providing adequate security and service assurance needs. Challenges such as slow lead times, potential refusal of rights-of-way, state and local citing laws, guarded community perspectives, and uncertain return rates in comparison to other investment needs produce hesitancy when considering security for the electrical infrastructure.

Restructuring facilities and increased competition could also modify a market participant's security incentives and responsibilities. These stakeholders vary by their amount of involvement, ability, and focus. Most electrical companies of today invest in protection that will not conflict with their resources or create customer disapproval. Oftentimes, security measures are supported through proposed rate or price increases. Current regulations, unfortunately, leave stakeholders with no guarantees of recovering the costs for mandated security.

Compounding the problem of protection is the issue of theft. As prices of copper skyrocket globally, thieves target utilities to steal copper from electrical substations and remove copper wire and cable, dismantling the network. This vandalism has become such a large problem that in 2009, the Electrical

Safety Foundation International (ESFi) estimated copper theft cost U.S. utilities more than $60 million annually.[3] In addition to utilities, other large power uses like rail transportation have similar theft problems.

Europe has faced a near overhaul of its railway systems due to copper theft, triggering large-scale disruption and loss profits as thieves target cables, signal boxes, and dynamos. According to Mineweb, in 2010, five operators stated that copper wire theft in Europe caused them more than 10,000 hours of train delays and damages estimated in the tens of millions of euros.[4]

2.2 Oil and Gas Industry

The oil and natural gas industries are segmented into several stages, including, oil production, crude oil transport, refinement, product transport and distribution, and external support systems. With this extensive staging process, infrastructure protection could take on many forms in facilitating each component of the industry, carrying with it a hefty price tag. One challenge for the oil and gas industry is determining and mitigating the extent and expense needed for proper security in the event of a terrorist attack or natural disaster.

Obstacles for this industry do not end at determining the appropriate preventative measures; several issues can arise once infrastructure is damaged during a critical event, increasing response and repair time. Obtaining construction permits and waivers from local, state, or federal government, as well as acquiring construction rights-of-way for pipeline placement on bordering properties could take several days of processing. Adhering to environmental impact laws, while still obtaining the necessary and sometimes sparse material and equipment needed, could decelerate the reconstruction process once infrastructure is damaged.[5]

2.3 Communications Industry

With the rapid and competitive technological advances of today's global market, the communications sector has become the chameleon of infrastructure as it constantly shifts to facilitate the most current needs and trends of society. Regardless of its shifting grounds, the communication industry has reliably responded to the needs of both large- and small-scale businesses and governments. Unfortunately, more innovation transmutes into more challenges. The instant availability of vast amounts of data creates new and substantial problems with securing both virtual and tangible critical assets. Governments and infrastructures across the globe utilize the communications industry to obtain essential information for its day-to-day operations, establishing imperative initiatives for sector protection.

The proliferation of the Internet creates threats to the communications industry – both natural and human-based. Severe weather, accidental cable cuts, and physical or cyber sabotage can be daunting for industry leaders to monitor at all times. It is important to address each real threat individually and establish protective measures to combat these continuously evolving issues.

The communication sector is the first responder and oftentimes, the first target when terrorists attempt to infiltrate key infrastructures by way of confusion. Clear protocol must be established to protect communications and prevent further damage to other sectors.

2.4 Water Utility Industry

Water, one of the most basic global elements, is used for complex and extensive solutions. The water utility industry tailors services for small groups, as well as populations ranging in the millions. The sector's key focus is managing fresh water supply and wastewater collection and treatment. In regard to fresh

water supply, CIP is geared toward public water systems reliant on reservoirs, dams, wells, and aquifers, as well as treatment facilities, pumping stations, aqueducts, and transmission pipelines. All humans require water to survive, and it is this universal need that makes water supply protection a global concern.

Due to a wide and diverse range of customers, water utility leaders concentrate their protection efforts at a high level – focusing on incidents that lead to considerable human death tolls, major property damage, and/or far-reaching economic losses. The sector's largest threats include deliberate contamination of the water supply by way of toxic chemicals, cyber attacks on electronic water management systems, or disruption of services due to varying factors from different infrastructures.

To tackle these fears, the water utility industry amplifies its monitoring and diagnostic systems to notice the first signs of any biological, chemical, or radiological toxins infiltrating the water supply. State and local methods for handling water facility emergencies differ in both strategy and procedure. It is important for local, state, and federal departments to collaborate emergency response methods when notifying the public of possible or actual water contamination. Public confidence is crucial to preserve in any industry, and customer relationships hinge on both the delivery and the promptness of key information during a crisis.

Water operations are highly dependent on other sectors, such as the electrical industry that provides running pumps and power for treatment facilities. The strong correlation between critical infrastructures, such as the electrical and water utility industries, gives justifiable grounds for establishing solid security measures across all utility and communication networks.[6]

3. Physical Security Information Management (PSIM), PSIM +

Each of the industry sectors has its own unique challenges for protection of their critical infrastructure. While each faces some unique challenges, what they have in common is the challenge of protecting a large expanse of geographically dispersed critical network assets and equipment, and the need to monitor and quickly act upon information that can be centrally collected and analyzed. Situational awareness is the term given to the ability to integrate a large amount of information within a common operational view and be able to quickly and appropriately react to a perceived threat. This awareness is key to meeting the objectives of any solution for the protection of critical infrastructure.

Physical Security Information Management (PSIM) are security solutions designed to aggregate, normalize, correlate, monitor, alert, analyze, and report on information from traditional physical security devices and systems, and provide a common view of the organizations' current posture as an aid to proactive resolution and response. The same solution that monitors the normal operations of the expansive network of critical infrastructure, sensing anomalies that may indicate a terrorist threat, also provides a solution to improve security and monitor the status of the network to counter thefts and vandalism.

Video analytic solutions play an important part in the PSIM program. Video analytics are designed to automate the monitoring and analysis of an overwhelming volume of captured video data, identify and track objects, analyze motion, and most importantly, alert the proper authorities when something relevant happens. This best-in-class video surveillance performance shifts into proactively managing and responding to situations as they unfold, rather than reactively figuring out what happened after the fact. According to Aberdeen group, best-in-class performers who have adopted video analytics as part of their physical security program spend approximately 67 percent less than all others on a per-camera basis.[7]

Additionally, their guard force is successfully assisting, prioritizing, and taking actions of five-times more alerts per camera per day. Control rooms typically have fewer video monitors than the number of video cameras feeding them, and in any case, there are simply not enough eyes to monitor and analyze the sheer volume of video data displayed. Humans have distractions and other duties, and cannot be expected to catch every event that may cause alarm. Furthermore, physical security is relegated to reviewing video surveillance footage and reconstructing events after an event has already occurred.

From a technology perspective, the issue of protecting critical infrastructure in terms of safety and security requires a system that monitors the security (perimeter and access control) of the critical infrastructure, is linked or integrated with a central command center or control room, and is able to develop security threats, as well as manage naturally occurring events. Such a system has a consistent sensor fusion element (perimeter and anti-intrusion sensors, video surveillance, monitoring of the normal equipment operating settings, etc.). The alarms are mostly generated by these sensors. A response to an event not only involves dispatching resources and messages to institutional operators, but also planning and creating scenarios.

There are four different operational phases involved:

1. **Detection** – The detection phase allows you to acquire, on an ad hoc basis, all the information concerning an object (asset), event, resources in the territory, and the specific status of physical dimensions to be kept under control. The detection phase also includes functions for integrating sensors and information. The integration capabilities offered by the platform play a vital role in providing support
2. **Assessment** – This phase requires a high-level analysis and interoperability capacity to be able to use all the data available according to standard or ad hoc procedures and rules. The platform must also be able to support the integration of modeling, which must be considered, by its nature, extremely dynamic. The human-machine interface must also be flexible enough

to support the use of the widest variety of visualization modes (2D, 3D, superimposed layer, etc.).

3. **Response** – This phase is closely integrated with the assessment phase while an event is unfolding. It requires functions capable of managing resources in the most efficient way possible.
4. **Mitigation and Recovery** – Once the emergency is over, the next phase involves mitigating and returning the situation to normal. All the operations, which are no longer emergencies but plans, are managed according to the estimated damage and intervention required to restore safety and productivity to the infrastructure.

When, physical security information management is integrated with the ability to effectively manage not only the assessment, but also the response and recovery, the solution becomes more than just PSIM. Intergraph addresses Physical Security Information Management, plus response, or PSIM+. It is this ability of complete and proactive assessment, response, and response management that makes PSIM+ an integrated information system solution that consists of four operational phases, as shown in Figure 1 below.

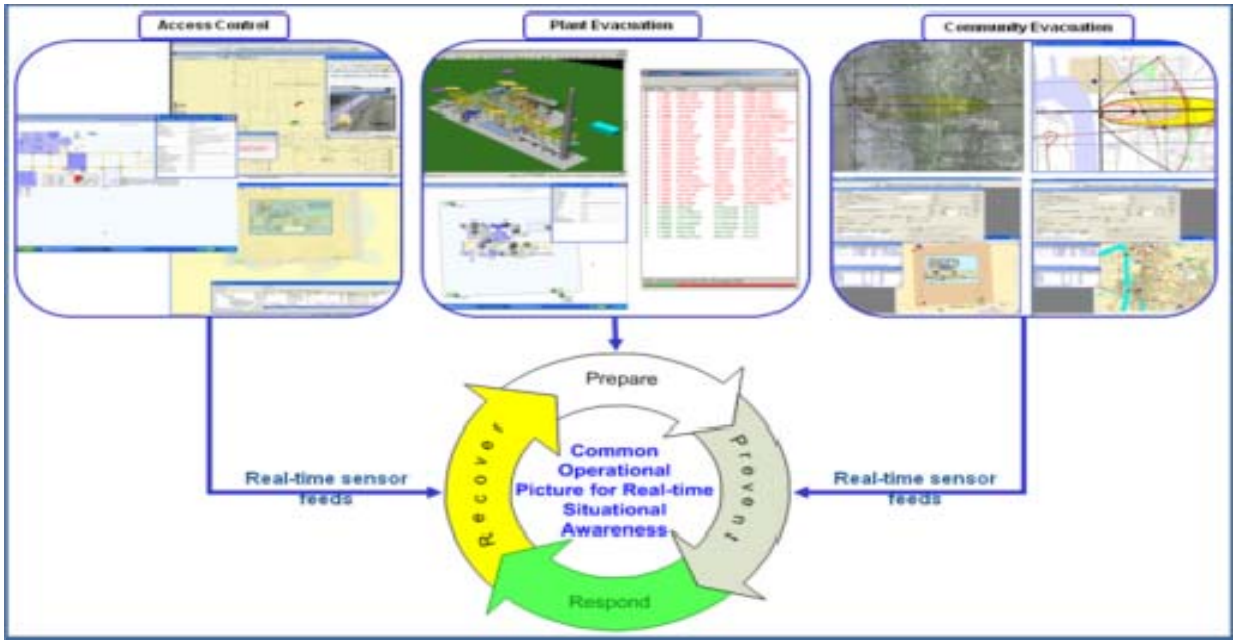

Figure 1: Four Operational Phases of Physical Security Process Management

The following factors determine the efficiency and response of a PSIM + solution:

- **High Scalability** – The solution must be available in different versions to facilitate specific user needs or process management. Migrating to higher versions should not require rewriting customized elements or any intervention on the previously processed data.
- **High Interoperability** – The solution should support different versions of interoperability specifications, such as the Open Geospatial Consortium (OGC®) for spatial data, which is crucial for visualization and situational awareness. Integration of these systems facilitate to specific standards.
- **High Usability** – The solution should allow data to be used via Web-connected and occasionally disconnected mode. In every case, the key importance of the data is respected regardless of the method of use.

4. The Solution: Intergraph's Critical Infrastructure Protection

4.1 Intergraph Computer Aided Dispatch (I/CAD)

Historically, Intergraph has been the leading innovator in the use of computer graphics and map displays for a command-and-control environment. In the early 1970s, Intergraph was the first company to develop a computer-aided dispatch system equipped with a cartographic interface based on a geographical database (Intergraph Computer Aided Dispatch – I/CAD). This system revolutionized situational awareness in command-and-control rooms by gradually expanding available decision-support tools. From its early versions, I/CAD has integrated the cartographic interface at both the database and communication level with specific modules for call-taking/handling and resource management, while still maintaining field workforce (i.e., dispatching integrated with the telecoms systems support vehicle-based and handheld terminals and remote and distributed access).

I/CAD is a distributed processing system that integrates conventional client/server architecture with Service Oriented Architecture (SOA) components. New developments obviously tend to be service-oriented, but the core of the call-taking and dispatching products comprises desktop applications that interact with the central database and other components using differentiated methods optimized for network access. See Figure 2 below for more information on I/CAD's abilities.

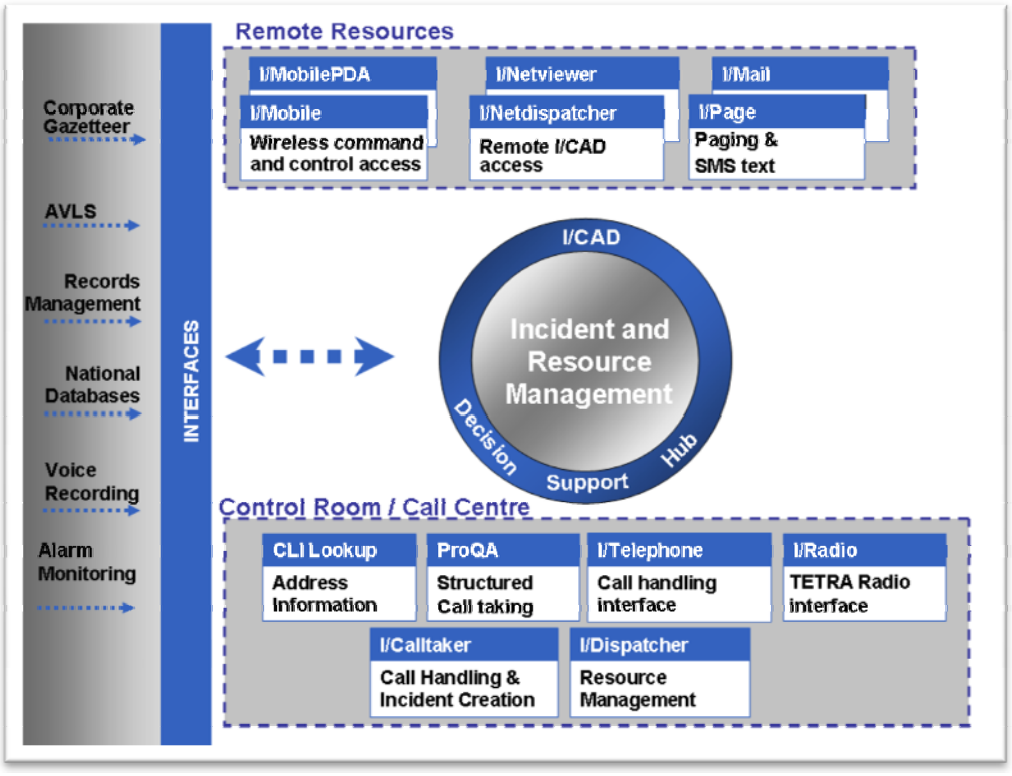

Figure 2: I/CAD: Total Intergraph Solution Based on Industrial Standards for Control Rooms

I/Executive is the operational product at the heart of the system, providing database management services and tools. It operates as the core of a high-reliability data infrastructure and focuses on data operations.

The I/CAD backend is comprised of redundant server systems (i.e., database server, application server, communication server). Depending on the required scalability, it can achieve a system availability rate of 99.999 percent and provide a disaster recovery solution operated remotely across the territory.

I/Calltaker and I/Dispatcher are the operational instruments deployed at control center level. Both tools share the same functional architecture for managing calls and creating incidents. I/Dispatcher includes additional features required to manage the resources and interface of mobile devices. Both products can interact functionally with essential services, such as emergency triage (ProQA) and those for verifying calls (EISEC/ALSEC).

Listener I/CAD completes the picture by offering a peer-to-peer communication protocol between components while keeping individual visualizations synchronized and up-to-date for new incidents, field events, and resource locations. Listener reduces database access to a minimum, thereby guaranteeing high scalability coefficients. It communicates using broadcast mechanisms that reduces network traffic and supports the distribution of I/CAD via local and geographic networks. To summarize, Listener helps create distributed sites by operating as proper “virtual control rooms.” Every operator has the chance to manage incidents and resources by using simple, intuitive commands for filtering only the relevant information in an area of expertise.

4.2 Intergraph I/Security Framework

Based on the highly reliable I/CAD backend, including both the dedicated server (dispatching and tracking) and database components for communication and the ergonomic features of the I/Dispatcher user interface, Intergraph has developed an intuitive control room solution for safety and security in critical infrastructures.

Unlike a rapid interventional operation room, where alarms are triggered by telephone calls, a safety and protection control room has alarms that are mostly triggered by sensors (perimeter control sensors, radar, intelligent CC-TV cameras, production-flow monitoring systems, etc.). The operator must be able to control the detection sensors (usually PTZ cameras) from a single, integrated environment and dispatch the response staff.

The cartographic interface of the situational picture requires all the functions of an advanced GIS application and must be able to quickly detect alarms, estimate positions of intruders or incidents (triggered by sensors), and locate positions of the response teams (equipped with GPS, AVL terminals, etc.). A GIS application with these features is defined as a common operational picture. The dataflow of the common operational picture is highlighted in Figure 3 below:

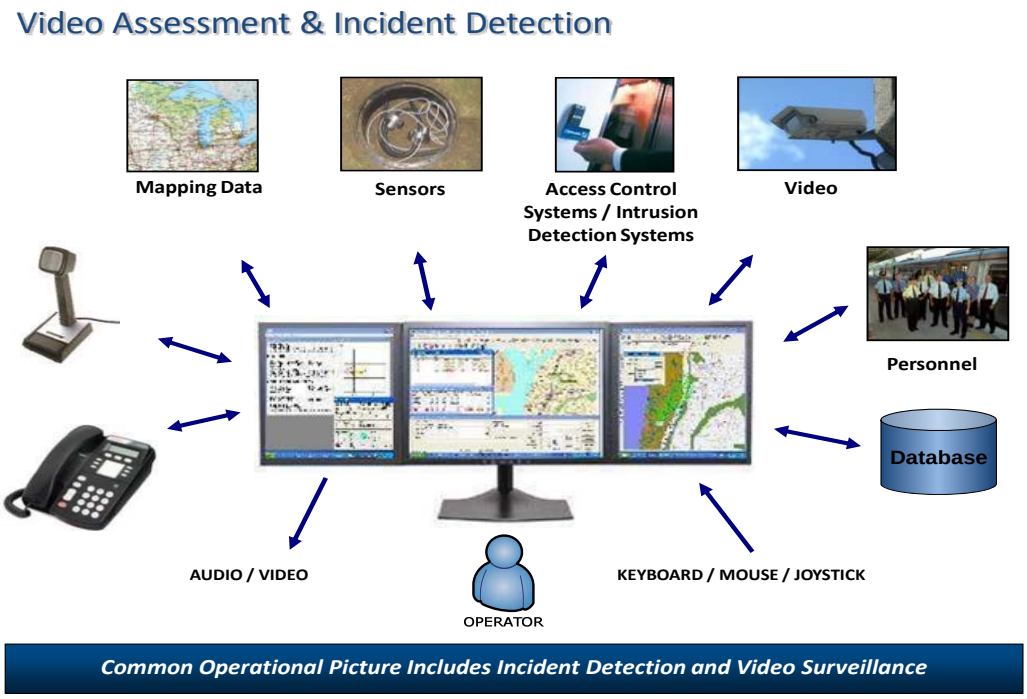

Figure 3: Common Operational Picture in Control Room Monitoring Infrastructure Safety and Protection

4.3 Intergraph Emergency Operations Center

The concept of a rapid intervention operation room evolved into an emergency operations center (EOC) in response to recent terrorist attacks and natural disasters. An EOC is a command-and-control center for crisis management, created in such a way that it secures against terrorist attacks and extreme natural events, with its own standalone power sources and telecoms systems. In keeping with the development of operational scenarios (terrorist attacks and climate disasters), an EOC operates both during crises and in times of peace. An EOC performs the following activities:

- Gathers, analyzes, and redistributes information
- Coordinates operational functions of command, control, and inter-agency
- Drafts and implements response plans for relevant scenarios

An EOC fulfills these tasks by having telecom systems, information fusion/common operational picture systems, geospatial intelligence systems, and call-taking/dispatching systems. While the goal of a rapid intervention operation room is to respond to events, an EOC uses a more complex data model based on the scenario and plan. The “operational” cartographic component is the common operational picture, and the resource management subsystem is, appropriately, a mobile resource management function (see Figure 4 below).

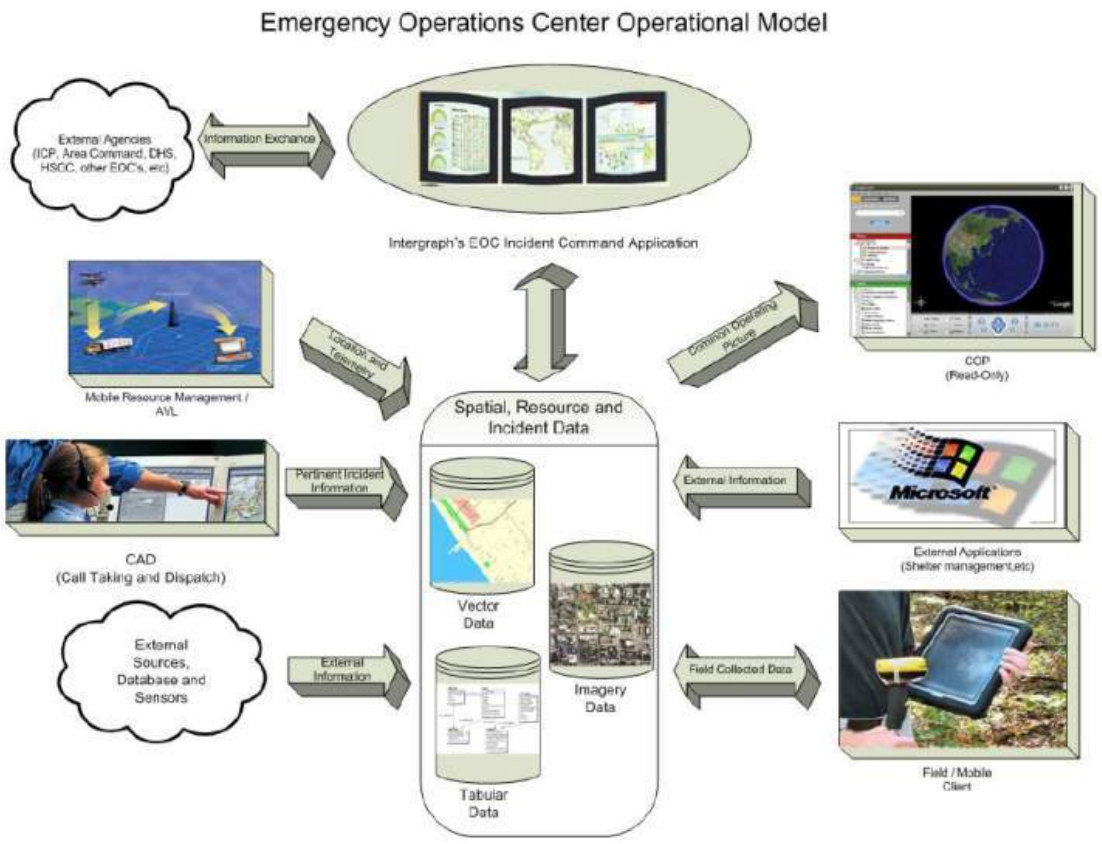

Figure 4: Functional Architecture of an Emergency Operations Center

The most critical requirement for an EOC is interoperability between the various agencies involved in handling a crisis. Each agency actually has its own technology systems with relevant data formats and specific operational procedures. This makes the problem both technical and organizational. To meet this requirement, Intergraph has collaborated with Louisiana State University, the U.S. Army Warfighter Protection Laboratory, Oak Ridge National Laboratory (ORNL), the U.S. Department of Homeland Security, and USNORTHCOM.

The result of this cooperation is an Intergraph software solution for EOCs that is operational at different U.S. federal sites and can support the U.S. operational standard NIMS (National Incident Management System) and the APCO (Association of Public Safety Communications) national standards. In addition, the Intergraph solutions comply with the critical information security standards of the U.S. DOD Information Assurance Certification and Accreditation Program (DIACAP) and the National Information Assurance Certification and Accreditation Process (NIACAP).

Intergraph is the first commercial manufacturer of computer-aided dispatch systems to be involved in the U.S. Unified Incident Command and Decision Support (UICDS) project. The UICDS project was launched by the Science and Technology Directorate of the U.S. Department of Homeland Security (prime contractor SAIC Science Applications International Corporation) with the aim of developing an interoperable architecture supporting multi-jurisdictional and multi-platform information sharing to boost rapid response capabilities and situational awareness in the event of a major incident.

Geodata interoperability is guaranteed by Intergraph's involvement in OGC and collaboration with Microsoft® and Oracle. By choosing interoperability architecture based on OGC Web services, the cartographic component, the common operational picture, becomes SOA-based, which often means it's accessible via a browser.

4.4 Intergraph for Infrastructure Management

A database describing industry-specific network infrastructure being monitored and protected is a fundamental component of a CIP solution. To optimize situational awareness for operating purposes, this component should be presented in a geographic context (i.e., determining asset locations, efficient deployment of field resources, etc.). It should also provide the basis for visualization and management of the asset network.

Intergraph offers an infrastructure management solution designed specifically for energy and communications companies. Integrated with the geographical database, it is designed to manage millions of discreet, connected network assets and is built for optimal graphic performance and scalability for any utility enterprise. Complete solutions are available to manage critical asset networks for the following industry sectors:

- Pipeline
- Gas
- Electric
- Water/Wastewater
- Heating
- Communications

Intergraph has developed a series of pre-configured solutions for each of these industry sectors based on more than 40 years of corporate experience with utilities and communication companies. These solutions are focused on meeting the requirements of any company, thereby guaranteeing maximum productivity within the entire system.

Figure 5 below depicts the system's overall architecture:

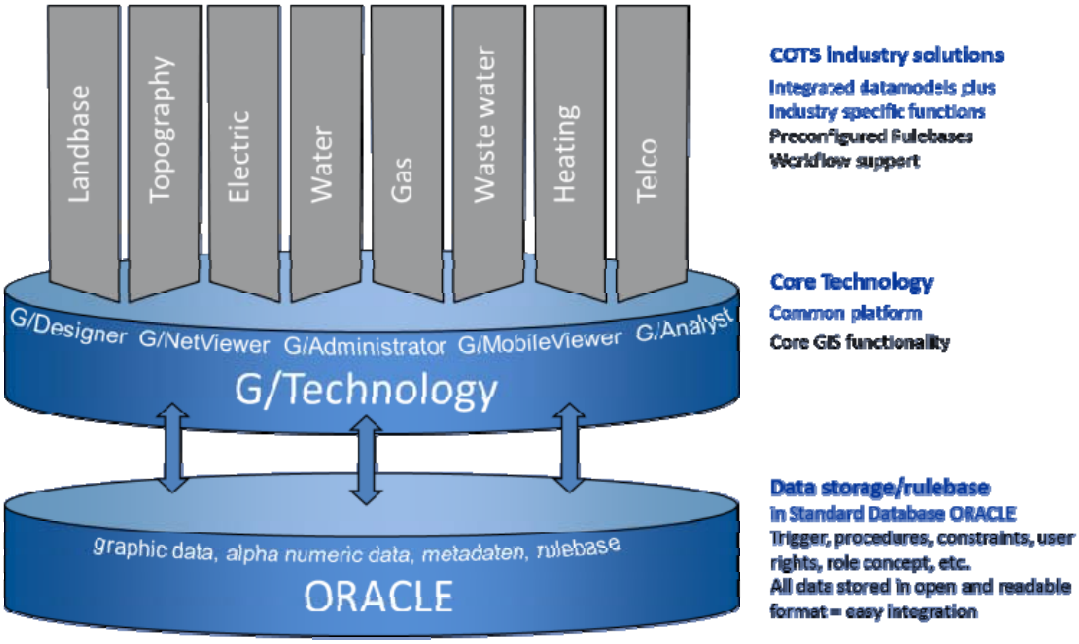

Figure 5: Overall Architecture for Intergraph's Infrastructure Management Solution

The reference technology platform is Intergraph's G/technology software and includes various industry-specific network infrastructure and design application modules. It offers a highly modular, powerful, and robust environment developed in accordance to OGC principles, which guarantees maximum openness and interoperability.

G/Technology's entire geometric component, the data model, network model, metadata infrastructure, and transaction management are archived and managed exclusively within an Oracle geospatial database. No middleware is required to visualize, access, or update the data. G/Technology can manage terabytes of data, as well as support thousands of concurrent users at any level of interaction (i.e., administration, design, Web, mobile, etc.).

Intergraph provides sector-specific, pre-configured data models as the starting point for quickly reaching initial operational capacity for a project. You can make customizations to the software configuration, as well as personalized adjustments and custom interfaces to improve operations and accelerate workflows. Every industry sector model includes the following:

- Equipment features
- Definition of the network and connectivity
- Management of relations and menus
- Data model construction and maintenance
- Physical configuration* of the network (electricity, gas, water, pipeline, and communications)

**Physical configuration includes identification and localization features and complete functions for maintaining and managing events that occur throughout the entire life cycle of the system.*

5. Intergraph's Critical Protective Solutions for Today's Critical Sector Needs

Protection of critical infrastructure is an important part of today's mission for energy companies such as utilities and communications providers. Threats of terrorist attacks and natural disasters are justifying factors for safety. It is the responsibility of every owner and operator to assess and adopt measures for appropriate infrastructure protection.

Countries across the globe, governments representing entire continents, and the majority of professional industry organizations have already mobilized to create industry security and critical infrastructure protection guidelines to mitigate these risks; however, it is clear that each market sector has difficulty in determining the appropriate level of investment. It has been said that, "Security is always excessive until it's not enough." Determining the required personnel, business processes, and systems to protect critical infrastructure are individual business decisions based on individual assessment of risk. Upholding a public image, as well as weighing in the direct and indirect economic impact of such decisions, are factors most businesses consider before deciding on the appropriate CIP levels.

Intergraph Corporation is uniquely positioned to provide fully integrated physical security information systems with integrated response capabilities (PSIM+). For more than 40 years, Intergraph has been developing comprehensive, commercial off-the-shelf software solutions based on industrial standards. Today, one out of every 12 people is protected by Intergraph systems. Intergraph provides a global benchmark in terms of efficiency and reliability for control rooms and operations centers dealing with critical infrastructure for utility and communications networks. Intergraph also provides solutions for CIP in the transportation, government, and public safety sectors.

Intergraph understands that to achieve actionable situational awareness, you need accurate, intelligent data, and you need it fast. Intergraph's CIP, mobile asset tracking, and geospatial intelligence solutions – built on standard, open technologies – provide domain awareness in day-to-day operations and emergency incidents, enabling joint interoperability, shared situational awareness, and the ability to execute highly synchronized mission operations. As a result, you'll have a common operational picture that integrates technology, sensors, communications, data, and more – giving you the advantage of real-time, integrated information from one central location.

References

1. *On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection*. Official Journal of the European Union. Council Directive. 23.12.2008. December 2008.
2. *Research and Markets: Increased Budgetary Allocations for Critical Infrastructure Protection Drive the Asia Pacific Oil and Gas Infrastructure Security Market.* Business Wire. Oct. 30, 2009.
3. *Copper Theft Baseline Survey of Utilities in the United States*. Electrical Safety Foundation International (ESFi), January 2009.
4. Vinocur, Nick; Kovalyova, Svetlana. *The Dark Side of Copper's Price Surge.* www.mineweb.com, April, 12 2011.
5. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Department of Homeland Security. United States Government, February 2003.
6. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Department of Homeland Security. United States Government, February 2003.
7. *The Eyes Have It: How Video Analytics is Driving a Proactive Approach to Physical Security*. Aberdeen Group. March 2010

For more information about Intergraph, visit our website at www.intergraph.com.

UAC-US-0046A-ENG