WHITE PAPER

Technology Insights for Emergency Operations Centers

INTERGRAPH®

Contents

1. Introduction

Emergency operations centers (EOCs) and decision-makers in those centers face a common set of technology challenges. To be effective, emergency operations systems must incorporate external sensors and systems, manage data, display it intelligently within the appropriate context, provide situational awareness, and support response planning, decision-making, asset control, and long-term analysis. Intergraph solutions support many of these requirements and take into account the many issues related to doctrine, technology, people, and economics.

2. Meeting Technology Challenges

Managing emergencies requires a decision-support system that incorporates data from external sources, allows proper manipulation and display in an appropriate context, provides tools for decision-making and controlling assets, and allows long-term recovery and analysis to improve future decision-making. Unfortunately, most systems fall far short of these capabilities. As emergency operations centers look to enhance their systems, today's global security concerns demand a closer examination of the technology issues involved in implementing a system that fully meets all requirements.

Intergraph has significant experience in delivering emergency operations systems that support decision-making over large geographic areas. For example, we supported the Naval District Washington in the National Capitol Region during and after their response to the Pentagon attacks of September, 2001, and provided the incident management system used by the Office of Unified Communications in Washington, D.C., during the inauguration of President Barack Obama in January, 2009. Drawing from this experience, this paper presents lessons learned about the key technology issues facing EOCs and possible solutions or responses.

Before the system design starts, responsible authorities must develop doctrine and policy that will guide system development and implementation. Developing technology in a vacuum, without integrating it into a strategic and tactical plan, is not only inefficient, but also dangerous. System development requires the formal identification of requirements, needs, capabilities, and other planning directives necessary for implementation. Employing sophisticated sensors, links, communications, and collaboration tools is useless unless there is a policy and plan for use, agreements among agencies and governments on use and control, and an overarching strategy to implement the system and decision-making process. These processes are inextricably linked to the technology and business model processes that drive the tools and tactics to implement the strategy. This paper does not outline the development of that doctrine or policy – it assumes that process is ongoing in tandem – but looks at how you can leverage technology to tackle a common set of issues found almost universally in EOCs today.

3. Data Input from External Sources

Data collected during an emergency is useful in combating a disaster only if it is available in real time, viewable in an appropriate operational display, and accessible at various levels of command. It is of even greater value if an organization can integrate it into a complete tactical and strategic picture that displays data from a variety of sources to enhance situational awareness for decision-makers. (See Figure 1.)

These three limiting scenarios have been found in post-event analysis and reconstruction related to real-time data assessment at typical EOCs:

1. Critical information was not available at any point in the event and adequate sensors were not in place to gather the information.

2. Critical information was not available to the command center. Despite local sensors being in place, the information never reached decision-makers.

3. Critical information was available and relayed to the command center, but never placed in context or displayed so operators could use it in real time.

Scenario one – sensors not in place – may continue to be a problem, though with proper planning and analysis, organizations can more effectively employ sensors and information-gathering systems within budgetary constraints to ensure they collect the most critical information in real time. Planning for and employing sensors should always be part of developing doctrine and a deployment plan. Unfortunately, in many cases, the information is available somewhere, but – as in scenario two – it does not arrive at the appropriate facility. Or – as in scenario three – once at the facility, it is not presented in a meaningful context so responsible parties can make effective decisions.

It is useful to look at an example. On September 11, 2001, the Federal Aviation Authority (FAA) knew aircraft had been hijacked, realized the hijacked aircraft were being used as manned cruise missiles, and was tracking a potentially hijacked air-craft out of the flight corridor on a clear trajectory for Washington, D.C. In this case, various centers had most of the data collected by distributed sensors and systems to know that an attack on Washington, D.C., was imminent and that the probable flight path included the White House, Capitol building, and the Pentagon. Despite this awareness, the responsible agencies could not make an effective decision in real time because the command-and-control system could not get all the key data to decision-makers in the context of imminent attack. The important point here is that despite a sophisticated, multibillion-dollar sensor system – including civilian and military air traffic control and federal agency intercommunications systems – none of the data was used to mitigate the attacks.

***Figure 1**: Decision support requires the incorporation of data from a variety of external sources.*

4. Data Management and Manipulation

An agency can avoid these scenarios only if it has the right data on hand to formulate a response. There are several key steps in making data readily available. The first steps are to determine what critical data is required, catalog all the available data, and then collect it. During our review of several command centers, we learned that data is frequently available from many sources at the command center, but is not being used. Standalone legacy systems often exist and are tied to external information and sensors, but the data from those sensors is usable only in a very limited context.

For example, standalone meteorological stations display wind velocity, temperature, and other parameters, but these sensors are not available to support displays or models that can use that information to predict the spread of a particulate or chemical plume. It is imperative early in the process to assess what legacy sensors and systems are already in place that can provide useful information from the field. These systems are strong candidates for integration into the framework of the data bus.

The next step is providing data conveniently through a data integration method. As a general principle, all data should be accessible through the common network bus or data bus. Wherever possible, data should be available in its most basic format for processing by systems and operators who may be only distantly related to the primary or normal function of the sensor. Where it is reasonable to do so, it is often advantageous to make raw data available so that new or planned systems can access that data. In some cases, it is prohibitively expensive or inappropriate to place raw data directly on the data bus, but some other derivative of that data source could be provided. For example, although it is not normally useful for air traffic control radar sensors to supply data to disaster management centers, if some form of that data – even the trajectory data – was available, decision-makers on September 11, 2001, would have had an integrated picture to help make decisions.

In our approach, wherever possible, all data – video, audio, telephonic switch, radio switch, intrusion sensors, infrastructure sensors, perimeter monitoring systems, etc. – are accessible throughout the system for authorized uses. What may normally be useful to a real-time camera monitoring system can be easily integrated into a post-sensor trip assessment or other systems. This is not to suggest that we store all types of data in a generic format. While there is a good argument to do so, the technology is not there today. We can allow a system to manipulate, store, and process its normal data, and let other systems that need the data recall and access it on the bus immediately for other uses.

Obviously, you will need to manage this data to make it useful. Relational databases that can either store data or index the location of data are key in this management structure. You can load some raw data and most post-processed and decision-point data directly into these databases. You may need to store less structured data, such as video or analog sensors, in other formats, but it can be immediately retrieved by metadata and indexes stored in the relational database.

5. Intelligent Organization and Display of Data

Once you have gathered the data and made it available through the system bus, it must be presented in an organized way to operators and decision-makers. The design must consider the realities of a human being's ability to process and assimilate information and make decisions based on that information. Failure to analyze and understand this human element often leads to creating impressive-looking displays and disaster management centers that are unmanageable and fail to meet the objectives.

For example, you may have a requirement to monitor a video surveillance system with 100 cameras. A commonly used approach is to provide banks of large-screen monitors with operators sitting at consoles scanning the monitors. This is very impressive to look at, but nearly useless in most cases. Extensive testing of operator performance and decision-making in this environment confirms that these systems are inefficient and have a high failure-to-detect rate, since even alert operators become bored, easily distracted, and soon fail to notice changes in the display. In short, operators quickly become mesmerized with data that has little interest or stimulation. This system may meet the technical monitoring requirement, but is it not useful in providing the desired security in real time.

A much better approach is to use some form of queuing, where the operators look at the display only because something has happened that draws their attention to that display. Advanced motion sensor technologies, or other sensors such as pressure, water level, etc., trigger the image review by an operator. After a few seconds of alert analysis, the operator confirms there is useful data or dismisses it. But during that time, the operator's full attention is focused on the queued display. (See Figure 2.)

***Figure 2**: A display that provides data in a queued format is most effective.*

6. Information Context

Once data is gathered, it must be put in a common operating picture, as well as in the correct context to be useful. The designer must consider that the context may change at each level of the decision- making tree. From the call-taker's or first responder's point of view, the context may be limited to the immediate area and local situation. The responders and controllers or dispatchers are worried about individual units, individual capabilities, and support of the local mission.

Farther up the chain, decision-makers need a different context that includes other potentially related events, overall regional capabilities, disposition of forces and assets, potential public impact, and other larger issues. Still higher up in the decision process, large-scale evacuations, state and federal coordination, public affairs, and mitigation is yet another context the data must support.

It is highly advantageous to have the same data feeding these various contextually based displays. It is also useful for the displays to look similar at each level to reduce the reorientation required for each one. High-level filters and control of the displayed information can help put the information in the right context at the right level.

Clearly, the amount of data available in a viable, integrated command center requires additional processing and organization to be useful. One method to organize information is to represent it in a format people are comfortable with and that models their real-world, everyday decision-making process. Representing the data in a geographic format is an excellent method that has achieved measureable success. A GIS system can rapidly organize and display useful data and convey vast amounts of information quickly to operators. (See Figure 3.)

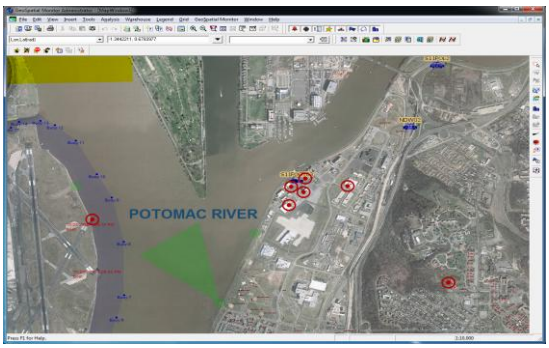

Figure 3: *A GIS provides information about assets and population in an easy-to-understand format.*

Operators are able to assimilate the information and then query for more detailed information. In the case of a disaster, where geography is critical to controlling the situation, geographic organization and display of the data can greatly assist in decision-making at all levels. From call-takers trying to assess the location of reported information, to the ultimate decision-maker for the allocation of resources, a common frame of reference in least understandable geography greatly improves the process and reduces the decision loop time in many cases.

Yet icons and graphical displays also have limits. They are excellent for quickly displaying 'big picture' data and correlating data, but they are not as good at providing detailed and text-based information. For this reason, it is important to provide data links to the most appropriate format. A good example is a graphical representation of a building on the map. The GIS map is an excellent format to show a building's location and relationship to other structures, but if details of the structure or other data are needed, text-based displays often work much better. Effective systems link these two together in a format that easily transitions from one display to the other.

Intelligent organization also implies grouping the data, particularly in text-based displays. There are a variety of available useful groupings, and the most useful may depend on the current situation. Good systems provide operators with the ability to regroup, sort, and organize data to present it in the most useful format.

7. Situational Awareness

At each level of decision-making, the operators and decision-makers must maintain situational awareness. The scope of that situational awareness changes from local tactical to regional tactical to strategic, but it is crucial that the appropriate situational awareness be available and useful to the operators. Decision-makers lose their ability to process new information and act on it if they cannot quickly put it in the context of the current situation.

For example, in the case of a toxic plume release, providing data to operators and decision-makers on the location of first responders, local inhabitants, and the geographic coordinates of the plume is critical. In the absence of situational awareness, they must assemble a picture of the event and its geography and geometry, location of forces, proximity to populations, and other information. A common operating picture can show the plume and its expansion, as well as the location of inhabitants and first responders in seconds, greatly shortening the decision loop time. In the case of a recent series of exercises, first responders were killed on two succeeding exercises because, although the data was available and was in the EOC in time, no one could put it in context and understand the situation quickly enough. Putting up a simple GIS large-screen display showing the local assets, units, plume, and local population density allowed decision makers to divert responders in time and prevent a subsequent disaster.

8. Execution of Preplanned Response

Preplanning is the hallmark of any successful emergency services group. There are multiple levels where you can incorporate preplanning into an integrated emergency operations system. At the lowest level, you can digitize existing preplans in document format and make them available to operators and decision-makers. More appropriately, you can build the preplans into computer-based checklists tied to events and queues in the system. In one system, detection of an anthrax case could trigger an anthrax medical pre-plan, while detection of multiple anthrax cases could trigger a bio-terrorism or weapons of mass destruction (WMD) preplan. Better yet, a system that is proactive, and not just an automated checklist, could handle more dynamic and difficult environments. A basic system of this type might use automated timers and alerts to queue operators of critical times. An even more advanced system would automate a rule-based architecture, artificial intelligence, or data mining techniques to assist in producing dynamic preplans in the planning and execution phases.

9. Decision-making Tools

Once an event is in progress, decision-makers require tools that can use all of the available sensor data, geographic information, archived data, preplan data, and other information to formulate a plan. These tools should not be standalone. Rather, they should be integrated into the data and display environment as seamlessly as possible. Looking again at the toxic plume release, one tool would evaluate the extent, propagation, and effect of the release and provide graphical displays of evacuation support infrastructure and impact on responding forces. This type of integrated tool can immediately produce meaningful input to decisions-makers while contributing to their situational awareness. It is critical, however, to provide real-time sensor data, such as wind conditions; historical data such as population and infrastructure requirements; chemical, radiological or biological data on the plume constituents; and other information as part of the model.

Once you have run the model, the output needs to be available immediately to operators and decision-makers. This is the absolute minimum to operate an emergency operations system in real time. The next step is to produce query and 'what if' modifications to the models. A simple example might be the number of possible deaths resulting from radiological exposure versus the number of deaths likely to occur during evacuation. This not only allows decision-makers to make better decisions, it also provides them with the support for their decisions decoupled from the emotional impact of the emergency.

Again, it is important to emphasize that whatever the tool is, its output must be meaningful and placed in context of the current situation. It is dangerous and misleading to reduce the output of complex simulations or models in decision-support tools to a simple number. Many decision failures occur because decision-makers used these simple outputs without understanding their validity or how they should be interpreted in the current context.

In a classic case, during Operation Desert Storm, computer models used by the Department of Defense predicted significant casualties of such a large magnitude that the estimated casualties often drove the tactical plans. The Department of Defense has undoubtedly the best modeling and decision-support tools in the world, yet the output of those models led to erroneous conclusions and decisions through-out the conflict. The underlying cause was not that the models were wrong for what they were designed to do; instead, the limitations of the models were not presented or explained to decision makers nor was the complexity of the results explained. In the interest of simplicity, all the data was reduced to a set of simple, single numbers, which were so over-simplified that they were invalid for the context at the time. The bottom line is that as these tools become increasingly complex and more capable, their outputs and controls must be tailored to provide a useful interface to help construct the optimum solution.

10. Integration of Organic and External Expertise

Another important element for the system is to integrate the expertise of local organic assets, as well as remote support. In most complex situations, there is local first responder expertise and a network of experts that can be tapped to provide additional support. Unfortunately, this second layer of expertise is usually remote and separate from the wealth of information, and situational awareness provided by the emergency operations system. These supporting experts frequently find themselves making decisions without the benefit of some critical information that is available locally, but no one knows to provide it.

A good system provides collaborative tools that allow these experts to communicate with decision-makers and have access to the local information. This collaboration should include – as a minimum – document sharing, check list sharing, white board reviews, situational awareness GIS displays, summary displays of capabilities requirements and conditions, and audio-video capability. Ideally, it is preferable to collaborate directly with first responders in a local incident command center to help eliminate inadvertent loss of data as the multiple layers relaying the information filters it.

Closely related to the need for collaboration with external sources and experts is collaboration with internal sources, who may perform their duties best when left at their local facility. There is a natural tendency to bring all local 'key players' to a large central facility, but while there are advantages to this approach, there are also at least two significant drawbacks. First, this pulls local leaders away from their own source of resources and talents. Often, the critical document or information leaders need is not at the emergency operations center, but at their home base of operations. Pulling the talent away from their base of operations can dilute their effectiveness and lead to delays in decisions and execution of response. Clearly some critical mass must reside in a central location, but others are most effective if not moved, assuming that real-time, reliable, and complete collaboration is available.

Second, in major metropolitan areas, it may be nearly impossible to get key personnel from their normal location to the EOC. Major disasters produce nearly instantaneous gridlock and congestion. During the transit time, which could be the most critical minutes and hours of the emergency, your key personnel and command elements cannot afford to be stuck in traffic.

11. Integration of External Command Centers and Capabilities

Collaboration with remote command centers is also vitally important, including the local incident command post. The ability to share information from on-scene commanders to decision-makers can greatly improve situational awareness and lead to much better decision loop times. One case that demonstrates the importance was the delay in the state of Florida in requesting emergency federal assistance after hurricane Andrew. With southeast Florida in ruins, the state government delayed for days in asking for federal assistance, because they lost the situational awareness with the local government. There was no effective collaboration and state officials failed to appreciate the urgency of the situation or the magnitude of the damage. They were fully aware of the numbers and figures of the disaster reports, but were unable to appreciate the meaning of those enormous numbers. Only after viewing the damage from an airplane did the governor appreciate the impact, and then he immediately requested federal support.

It is important to realize that collaboration is not limited to videoconferencing. The best videoconference tools display only images, pictures, and voice. More collaboration usually needs to occur, including sharing of documents, views into the situational awareness system, exchange of data, and potentially remote monitoring. It is also important that the tools for doing this be integrated into an intuitive and familiar common operating picture. People work best and make the best decisions in environments they are comfortable with. The paradigm employed by the collaboration tools should reinforce that environment, not detract from it.

One very successful approach is to use a place-based environment. This collaboration environment uses common models and reference points such as virtual facilities and systems. You can hold meetings in virtual rooms, pass around documents, and make private and public exchanges, all following normal rules of business behavior enforced by software. This type of framework offers the value of collaboration without the penalty of unfamiliar and uncomfortable technology.

12. Command and Control of Assets

After making decisions, it is essential to deliver those decisions to the assets that will implement them. In many areas, extensive public safety radio systems provide the voice coverage to implement the delivery of these orders, but again, first responders are then removed from the situational awareness and sensor data loop. Mobile computing devices and PDAs can provide integration back into this world, but implementation of these devices must be thoughtful to provide contextually valuable and useful information without burdening the operators with extraneous data.

A good design summarizes critical data and then provides the tools to query for more information when it is appropriate. Additionally, the incident command system at the local command post controls many assets. The ability of this command post to communicate collaboratively with the emergency operations group greatly expands the effectiveness of each layer in the decision-making process.

13. Data Recovery and Long-term Analysis

The final key elements involving archiving, storage, and analysis, are the ones frequently underfunded, not implemented, or not used until the next disaster happens. There are two critical reasons to archive and store data and make it readily available. The first occurs during the event or disaster itself. After the initial fog of confusion begins to die down, it is crucial to review what the actual conditions are and what has actually been done. It is almost certain that something ordered or believed ordered by key decision-makers was not completed during the initial confusion.

Once you achieve steady conditions, it is still important that near-term data be immediately available. Questions such as, “What exactly did the caller say?,” “Where did the response team initially go?,” “What were all the initial alarms?,” and “May I see that picture again?,” are all valid ones that the system must be able to instantly provide.

Equally important are the weeks, months, and years following the incident. The more we learn from events, the better prepared we will be in the future. Each event is an opportunity to improve doctrine, procedures, training, or policy. This data is also important for future research by others and may provide the critical support for funding and system modifications. A robust system should be built from the ground up to support this requirement, or it will fail to take advantage of the most valuable design information of all – real-world performance under enormous system and human pressure.

14. Conclusion

The best approach to developing an emergency operations system is to support doctrine and policy, and not just automate or enhance current processes. Integration of technologies and applications is a key element of success, but the design must support the needs of the various levels of users. The requirement is to provide meaningful information in a common operating picture so decision-makers at all levels can make appropriate decisions during high-activity times. Throughout the introduction of technology, an implementation approach that incrementally deploys applications to support the doctrine and policy and evolves as appropriate has proven to be the most successful. Too many times, people look at technology as the panacea to solve all problems. Intergraph's approach is to engineer a solution that takes into account doctrine, technology, people, and economics.

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

Intergraph is a wholly owned subsidiary of Hexagon AB, (Nordic exchange: HEXA B) and (Swiss exchange: HEXN). For more information, visit www.intergraph.com and www.hexagon.se.

©2011 Intergraph Corporation. All rights reserved. Intergraph and the Intergraph logo are registered trademarks of Intergraph Corporation or its subsidiaries in the United States and in other countries. Other products and brand names are trademarks of their respective owners.
PSF-US-0077A-ENG 3/11