

Solutions for Safe Cities

Concepts for Integrated Operations Centers

Contents

1. Smart City/Safe City: The Need for Integrated Operations Centers	1
2. Issues and Pain Points	2
3. A Model for an Integrated Operations Center Framework.....	3
3.1. What’s happening?	3
3.2. What might happen next?.....	4
3.3. What’s my next step, what tool and resources do I need, who needs to know?	5
3.4. How well did I do?	6
4. Integrated Operations Center	7
5. Conclusion: What will success look like?	9

1. Smart City/Safe City: The Need for Integrated Operations Centers

In the last two to three years, a number of countries have experienced natural and human-induced disasters, including in the Asia-Pacific region New Zealand, Japan, and Australia. Inquiries into the devastating Black Saturday bushfires in Victoria during 2009, and the 2011 floods in Victoria and Queensland, have provided case studies highlighting the problems that can arise when operations centers for disaster management are not integrated.

The Victorian Bushfires Royal Commission Final Report Summary¹ determined there was confusion about responsibilities and accountabilities, and that the separate technology systems of the two lead agencies led to duplication of functions within the operation. It further highlighted the need for officers “to be supported by robust, consistent and coordinated information and systems.” A year later, the Interim Report into the 2010-2011 Victorian floods made similar observations: there was confusion about who was in charge; a disconnect between the integrated control centers (ICC) and municipal emergency coordination centers (MECC) such that local knowledge was ignored or discounted; updates and information were difficult to obtain; and there was no common operational IT platform in place to support an integrated multi-agency response².

While these reports focus on natural disasters, similar reports from elsewhere in the world may also focus on a terrorism event (for example, the Mumbai bombings or the Oslo shootings), or civil unrest (for example, the UK riots). Rather than look at how such incidents are managed in isolation or silos, there is an increasing need to deliver an “all hazards, all agencies” integrated operations system. Additionally, an integrated operations system must be able to manage planned as well as unplanned events, and have the ability to escalate from a planned event to an unplanned incident rapidly and smoothly. An “all hazards, all agencies” approach has a requirement for a single management authority that is able to view the big picture and remove the silos of information and operation that can inhibit response and recovery. Such an authority needs complete situational awareness where timely and relevant information is presented to stakeholders in a form that makes sense to each individual, without overloading them with unnecessary detail.

The ramifications of a disaster or citizen safety situation can extend well beyond the immediate timeframe of the emergency and its response. Consideration must be given to ongoing business continuity in fuel and energy supplies, access to shelters and temporary accommodation, food and fresh water, and medical supplies and resources. The resiliency of the community is strongly dependent on this continuity, and collaboration with agencies other than traditional emergency services – health, human services, public and private utilities, and charitable organizations – is nearly always necessary.

An Integrated Operations Center (IOC) brings responding agencies and systems together on a common operational platform that supports sharing of information and collaborative decision-making. Such a center is the foundation of the concept of a Smart City/Safe City where detection, prediction and information management technologies are fused into the common operating picture (COP). Integrated operations means no longer having separate solutions and processes for natural or human-induced disasters, terrorism and security, citizen safety and large-scale pre-planned events. Integrated operations also refers to the ability to draw on both organic and remote expertise and assistance, and to share information with experts in order for them to assist decision-makers.

¹ Teague, B, McLeod, R and Pascoe, S (2010). 2009 Victorian Bushfires Royal Commission Final Report: Summary

² Comrie, N (2011). Review of the 2010-11 Flood Warnings & Response

2. Issues and Pain Points

During both planned and unplanned events participating agencies can often only make decisions based on their own viewpoint. They utilize information from their traditional data sources but this can limit their ability to see an unfolding situation in its wider context. A spatial data infrastructure-based solution combines traditional and non-traditional spatial and spatial-like data into a single, cohesive and comprehensive view that can be tailored and filtered according to the needs of each user. Non-traditional data sources include information from sensory devices such as heat and motion sensors, fixed and motion video, and video-based behavior analysis and intrusion detection.

It can also often be the case that no one agency has a complete visualization of their necessary and available resources/tools, or those of allied emergency response agencies, and is not always prepared for a collaborative response. An interoperability capability allows resource information and tools to be presented to users in the context of the developing disaster or citizen safety scenario, enhancing their situational awareness. Knowing where all resources and tools are at any point in time allows for a faster, more accurate response that considers all aspects of the situation's environment.

This COP allows emergency services and other government and non-government agencies to have a common view of the disaster or emergency situation and allows them to make more accurate and timely decisions together. The enhanced situational awareness delivered by this COP allows stakeholders to see all parts of the jigsaw puzzle.

Rarely does such an event, planned or unplanned, involve only a single responding agency. However legislation and operational processes mean that agencies operate in silos and are not always able to share information necessary for collaborative decision-making. Shared planning and response tools enable responding agencies to make collaborative operational decisions based on their COP. Allowing information to be shared and allowing the agencies to use the shared information provides for timely and accurate decision making in response to emergencies and disasters. This desire to share information across agencies however can give rise to political and legal complications. A balance must be found between privacy and response, and between security of information and the need to know. A further issue faced by responding agencies is that legislated power to operate together and share data often lags behind technological capability. Robust, credential-based identity management, using industry-standard access mechanisms, allows sensitive information to be shared only with trusted users. Allowing only necessary information to be shared with trusted personnel provides for the balancing of operational needs against sensitivity and privacy.

Integrated operations systems can be inflexible, hard to use and maintain, and lack the adaptability needed in an "all hazards" context. An integrated operations and data sharing platform utilizes open standards for data exchange, is driven by familiar personal computing user interactions, and delivers data in real time avoiding the need for operators to guess at what is occurring. Information overload is avoided through role-based tailored presentation of material and an appropriate level of interaction. In this way operator training costs are reduced, and operations can be ramped up quickly in the event of an emergency or escalation. Capability of integrated operations center and the expectations of their users can exceed the financial capacity of agencies or governments to deliver them. It is therefore important that solutions are able to demonstrate real value, and that costly re-work of systems is avoided as regional and global conditions change over time.

3. A Model for an Integrated Operations Center Framework

In business – as well as life in general – achieving an outcome relies on a “Model for Change,” often stated in simple terms such as these.

- Where am I?
- Where do I want to be (and how will I know when I've arrived)?
- How do I get there?

This relatively unsophisticated change model (Figure 1) forms a basis for understanding the framework into which Integrated Operations Center solutions fit, as it guides the steps that must be taken to detect, respond and recover from a natural or human-induced disaster.

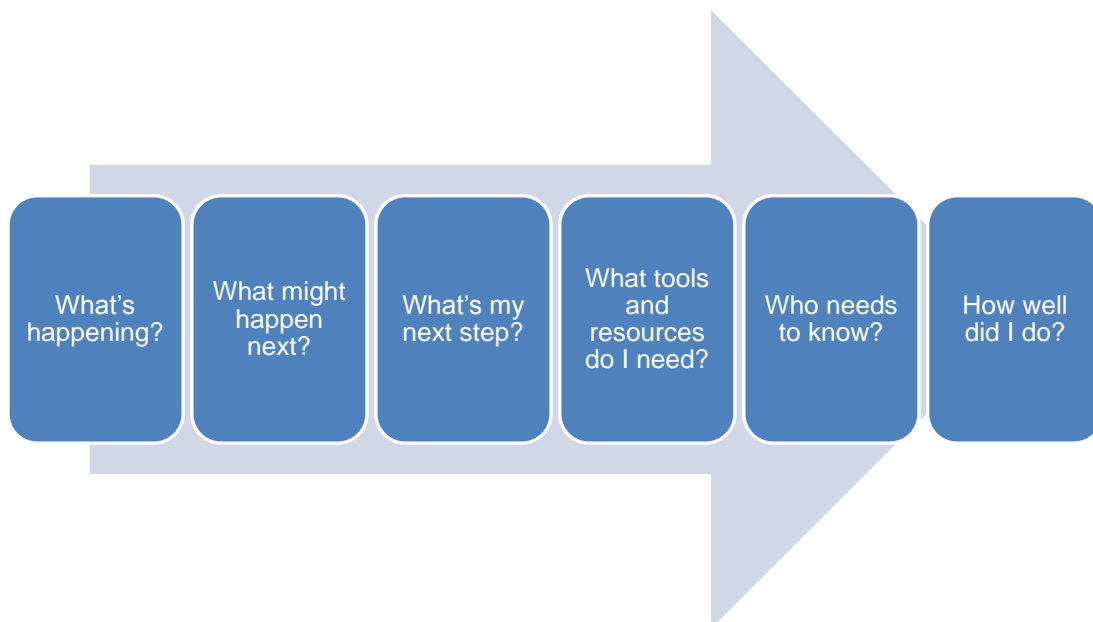


Figure 1: A model for change answers questions such as these.

3.1. What's happening?

Detecting possible triggers for an incident and monitoring an incident as it progresses are the first steps in integrated operations. This ability to detect and monitor the event, and present that information in its correct context is necessary for repeatable, collaborative decision making.

Processing large amounts of data about an unfolding situation and presenting it to stakeholders in its correct spatial context is an important foundation of integrated operations. Examples of the data sources that might be available include:

- Two and three dimensional spatial data including aerial and satellite imagery
- Three dimensional models of infrastructure
- Visualization of emergency calls for service, resource and other asset locations
- Fixed and motion video streams in their correct spatial context, tied to behavior analysis or intrusion detection systems

- Alarms and other triggers
- Sensory data from radar, motion, CBNRE and other sensor types
- Meteorological data
- Traffic and crowd congestion

While some of these data sources are from those traditionally accessed by emergency services, the “all hazards, all agencies” approach means that the increasing number of data sources to be integrated belong to both public and private organizations. This diversity raises two critical issues. Firstly, data sources need to conform to established or recognized standards. The Open Geospatial Consortium (OGC) of which Intergraph is a foundation member develops and promotes interoperability standards for geospatial data. This is especially important for non-traditional data, both cartographic and non-cartographic, such as sensory information through SensorNet or Sensor Web.

Developed at the Oak Ridge National Laboratory in Tennessee, SensorNet is a collection of systems for the detection and assessment of CBNRE (chemical, biological, nuclear, radiological and explosive) threats, delivering standards-compliant streams of data to the IOC systems³. The Fort Bragg military complex in North Carolina is an example of its installation, and combined with the Intergraph integrated security and computer-aided dispatch system, delivers a whole of life-cycle emergency management and citizen safety solution. Fort Bragg has a resident population of many thousands of military and civilian personnel.

Secondly, with the ability to share information from a variety of sources, there must now be a balance between the competing issues of privacy and response, and between security and need-to-know. Technology is able to assist in the protection of sensitive information through identity management and the establishing of trust relationships between systems. Information sharing is therefore rules-based and ensures that only credentialed users have access to the sensitive data that is needed for their own decision-making.

Unfortunately the time when all hardware and software systems conform to common data standards is still a long way off. Until then, and while existing hardware and software systems must be integrated into the operations system, the intelligent convergence of these devices, systems and networks is an important requirement. Middleware solutions such as Augusta Systems' EdgeFrontier[®] enable non-programmatic interfaces to be developed and deployed rapidly and cost-effectively, and improve operational efficiency through automation, filtering and event processing.

Situational Awareness is the ability for all stakeholders in an emergency or planned event scenario to have a complete, up-to-date and consistent view of the unfolding situation. This COP allows all decision makers to exercise their command, based on the information being presented to them, knowing that the operational decisions they make will be consistent with decisions being made by other operational authorities.

3.2. What might happen next?

In order to determine the decisions to be made and the steps to be taken, we need to understand the possible future states of the event. Prediction technologies take the current state of the event and provide users with one or more possible outcomes given the forces at work that may influence those outcomes. Spatial data is again key as terrain, hydrology, vegetation, infrastructure, and current and forecast meteorological conditions can all influence predicted outcomes. The prediction models give the likelihood and timing of each possible outcome so that responding agencies are able to prepare for them.

³ http://www.ornl.gov/info/press_releases/get_press_release.cfm?ReleaseNumber=mr20060215-00

Examples of prediction models include:

- Fire front direction and speed, with effects of spotting and ember attack being recent refinements to these models⁴
- Flood and other hydrological modeling
- Chemical and smoke plume drift⁵
- Vehicular and foot traffic movement and likely congestion points
- Radio line of sight and view-shed modeling

In order to get the results of these models to all stakeholders for decision-making and resource allocation, their outputs must conform to accepted GIS standards. They are run once from a single location, using the current conditions as known at the time, and made available immediately to necessary personnel. The challenge is to ensure that developers of these tools know of and understand these data sharing standards, and design their tools to be integrated into IOC systems.

3.3. What's my next step, what tool and resources do I need, who needs to know?

Integrated decision support systems enable operational personnel to execute pre-planned processes and procedures, and provide notifications to stakeholders external to the integrated operations center. Procedures and processes must be built on recognized frameworks such as NIMS (National Incident Management System) in the US and AIIMS (Australasian Inter-agency Incident Management System) in Australia and New Zealand.

The business rules that form part of these procedures will determine what resources, tools and assets are required to execute the next step or steps in the event management process. Situational awareness is required in real time to highlight the location and status of resources, the location and quantity of available assets (both consumable and non-consumable). Notification processes determine who must be given responsibility for the execution of those steps, and when and how they are to be notified. In many cases the processes and procedures that are being followed also mandate the content of a notification.

These procedures will also determine who must be notified in the event of an escalation of the event.

Integration with computer-aided dispatch (CAD) tools ties the IOC with the command and control of resources for dispatch and management throughout the event lifecycle. The availability of such resources must be carefully managed, especially human resources that may become fatigued or emotionally strained by the situation. CAD tools deliver spatial and tabular information about these resources, and through the use of mobile data resource managers and supervisors are able to exchange information, identify the most suitable resources for an activity, and direct them to that activity or location. In return resources must be able to update the IOC with their current location and status so that the next resource allocation decision is driven by the most up to date information.

Collaboration tools such as Microsoft® SharePoint® enable document exchange and management, and the delivery of timely information to stakeholders external to the IOC through private or public web portals. External stakeholders include the public, media, government officials and senior management of responding agencies. The content and timing of information releases forms part of the event management chronology and will be used for post-incident analysis and review. Where expertise is sought from outside

⁴ For example, "Phoenix RapidFire" developed by the Bushfire CRC

⁵ An example is the Aloha plume and vapour dispersion model developed by the NOAA

the IOC collaboration tools allow internal and external experts to share information and insights into the situation.

Finally, whether an event is a security incident directly targeting critical infrastructure or that infrastructure is impacted by the event, those responsible for operating and managing it need to be alerted to any possible impacts, and be able to report on its status to the IOC personnel. It is important therefore that these contact details are up-to-date and accessible. Roads, railways, water, gas and electrical utilities are nearly always spatial in nature; if the management information is tied to the spatial data display in the IOC personnel can quickly establish who needs to be informed, and how, when such infrastructure is threatened.

3.4. How well did I do?

It is always necessary to look at an operation, whether planned or unplanned, in retrospect and examine how the event was managed. The spatial and textual/tabular data collected allows an appreciation of what was done correctly, an opportunity to review any mistakes, and to improve processes and procedures for when a similar event occurs in the future.

The spatial and chronological analysis of information is a powerful tool to demonstrate the relationship between actions within the event or incident and the drivers of their outcomes.

4. Integrated Operations Center

The concept of the Integrated Operations Center (IOC) is the combination of command and control, data visualization and sensor integration technologies into a common operating picture that improves whole communities' response to and management of planned and unplanned events, and builds the capability and resiliency of agencies charged with citizen safety, infrastructure protection, and relief activities. See Figure 2.

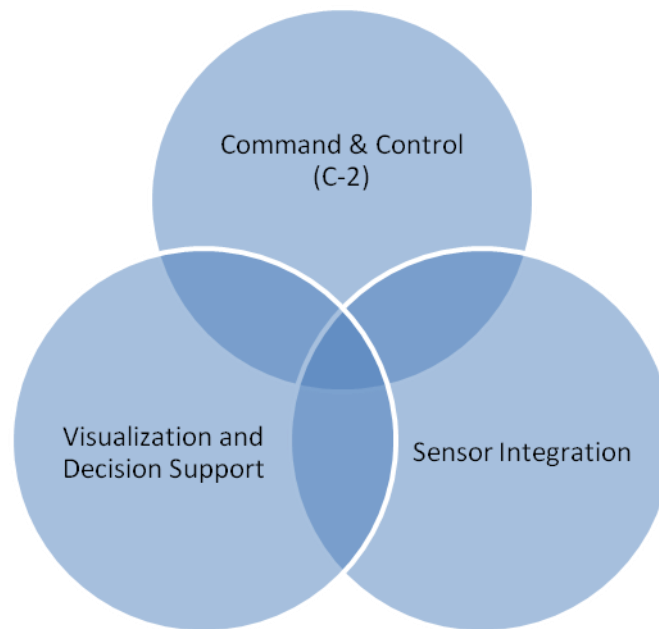


Figure 2: An IOC combines command and control, data visualization and sensor integration technologies into a common operating picture.

The IOC technology platform and capability enables diverse information sources to be shared and used for accurate and timely decision-making. It allows responding agencies to take advantage of detection and prediction technologies that can use all available and relevant data, and support decision-making in the wider context of the situation as it is now and as it might unfold. It is a virtual environment that provides operational support for an organization during normal and emergency conditions and accomplishes the following:

- Integrity between doctrine, policy and technology
- Access to data from external sources (sensor, video, other systems)
- Intelligent organization and display of data
- Information context
- Situational Awareness
- Execution and tracking of pre-planned response
- Decision making/support tools
- Integration of organic and inorganic expertise
- Integration of external command centers and capabilities to achieve unity of command
- Command and control of assets

- Data recovery and long term analysis

The IOC is a network-centric COP that allows all authorized echelons to have situational awareness and provides them with the ability to adapt to changes in the environment in real time.

The IOC may be staffed continuously, or opened only when required by operational procedures. The latter situation means that the center and the personnel that will be running it need to be ready at short notice. This in turn implies that the IOC technology platform must be cost-effective to maintain and the need for complex staff training and retraining kept to a minimum.

The integrated operations center allows responding agencies to:

- See and make sense of what's happening.
- Utilize a shared platform for collaborative decision-making.
- Cooperatively manage tools and resources, allocate tasks, and issue notifications.

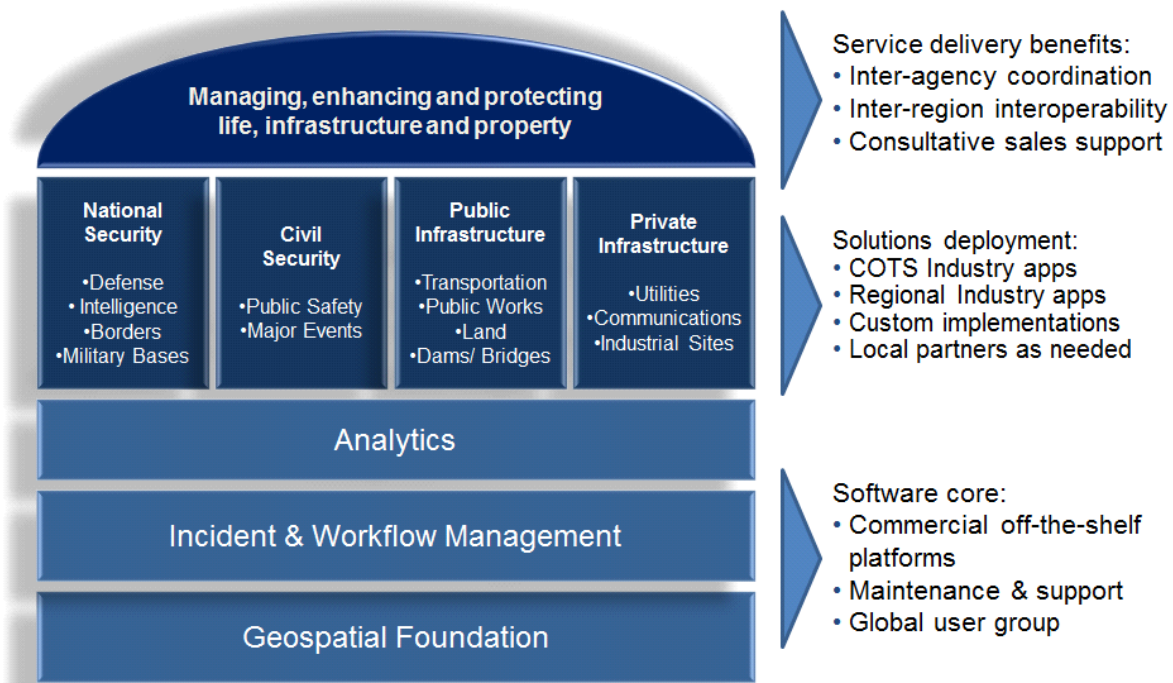


Figure 3: The IOC ultimately helps organizations manage, enhance, and protect life, infrastructure, and property.

5. Conclusion: What will success look like?

The success of an integrated operations center will be measured by the ability of decision-makers to have access to the information they need to allow them to make decisions in collaboration with other decision-makers and stakeholders. They will be presented with their own tailored views or slices of the common operating picture, updated and refreshed together with the views of other operators throughout the solution. Access to sensitive information will be managed through robust identity management and formal trust relationships that are aligned with legislated powers.

The integrated operations center solution will deliver value through its flexibility and ability to be maintained cost-effectively. Familiar user interactions with the system will reduce operator training and retraining, and allow the solution to be either used continuously or activated quickly when circumstances and procedures require it.

Intelligent convergence of spatial and non-spatial data from multiple traditional and non-traditional sources, either through shared data standards or through middleware solutions, will deliver a common platform for decision-making. Responding agencies can then make their necessary operational decisions in collaboration with their partners, and avoid the silos of operation that can hinder an “all hazards, all agencies” approach to the response and recovery from a natural or human-induced emergency.

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.com

Intergraph and the Intergraph logo are registered trademarks of Intergraph Corporation or its subsidiaries in the United States and in other countries. Microsoft and SharePoint are registered trademarks of Microsoft Corporation. Other brands and product names are trademarks of their respective owners. ©2011 Intergraph Corporation. All Rights Reserved. 11/11 SGI-US-0046A-ENG