

Achieving Operational Interoperability Through Emerging Standards

Contents

1. Introduction	1
2. The Evolution of Interoperability	2
2.1. Events That Have Driven the Need for Interoperability	2
3. Interoperability Concepts.....	4
4. Today's Emerging Standards	5
4.1. OGC Standards	5
4.2. Spatial Data Infrastructure and INSPIRE	5
4.3 The IJIS Institute and NIEM.....	6
5. Beyond Map Data and the Support of a Sensor Network.....	8
6. A European Program: Emergency Support System	9
7. DHS Unified Command and Decision Support.....	10
7.1 UICDS Technology Providers.....	11
8. Conclusion	12

1. Introduction

The term “security” relates to many disciplines that range from physical security to cyber security to national or homeland security. As technologies and applications evolve from using proprietary, binary data protocols to open, Internet Protocol (IP)-based data protocols, the convergence of these disciplines is happening at a rapid rate. Data standards are emerging that enable organizations to integrate data from various systems into information that can be used for tactical actions. Systems from one organization will be able to exchange information with systems of another organization to achieve operational interoperability.

First let’s define what we mean by operational interoperability in the public safety and security environment. For the purposes of this paper, interoperability is defined as the ability of a system or product to work with other systems or products without special effort on the part of the customer to enable:

- The ability to exchange and use information
- Networking with other networks
- Communication with another device
- One computer system to control another
- Systems to operate together with complete compatibility
- Diverse systems to work together effectively
- Multiple machines from multiple vendors to communicate
- Seamless interconnection of distinct systems

2. The Evolution of Interoperability

Technological advancements provide the means for solving problems, but in doing so, set up new challenges. With the advent of the first radio dispatch system for a police call in Detroit in 1928, radios have been the backbone of emergency communications. They became so valuable and prevalent that spectrum availability became a challenge. A solution to this was trunked radio. Trunking provided a means to achieve more capacity on the same set of channels. As in many cases, technology solved a problem, but also created more demand. Converting from analog to digital transmissions provided another technology leap to provide more capacity on the wireless networks. This, however, created a major problem in that radio vendors created their own over-the-air digital protocols, creating major radio interoperability issues. APCO Project 25 and Tetra are two standards that mitigate the interoperability issue with digital trunked radios.

Telephones introduced the capability for citizens to call for help quicker than in the days of needing to have someone physically run to the authorities. In the days of telephone operators, a caller simply had to dial 0 and ask for the call to be routed to the proper agency for help. As our telephone systems advanced and became saturated, human operators could not keep up with demand, and mechanical switches were put in place. The resulting problem for emergency calls was that people had to remember discrete phone numbers for the agency they needed.

In the 1930s, the UK solved the problem of remembering specific agency phone numbers by introducing the first three-digit emergency number, followed by Canada in the late 1950s. In the U.S., the first 9-1-1 call was made in Haleyville, Alabama, in 1968. These three-digit numbers provided callers an easier way to quickly request help. The introduction of digital switches provided additional capacity on the telephone networks, and the advent of selective routing helped get emergency calls to their proper answering points, while providing an address and phone number to the call-taker to aid in the response.

Finally, the ubiquitous cell phone came on the scene and became the primary means for people to call for help. The current wire-line technology was not able to route wireless calls, so additional technology was employed to solve that issue.

The technologies mentioned represent only those related to the caller and the responder. As needs evolve, the larger challenge lies in the ability for agencies and organizations to coordinate a response to a major event. As you can see, technology has provided easier ways for citizens to call for help and get the correct aid through call routing, location technologies, and computer applications. Communicating with responders to render aid to these calls for service has been enabled by evolving radio communications. As part of this evolution, agencies have begun consolidating in various parts of the world to achieve operational efficiencies and leverage their investments in the supporting technologies. This has solved part of the problem, but cross-agency communication and collaboration during emergency response remains a challenge today.

2.1. Events That Have Driven the Need for Interoperability

The global community has increasingly higher expectations for what governments should do to provide for their public safety and security. Evolution in technology has shortened response times, rendered medical aid at the scene of critical incidents, increased search and recovery success rates, and greatly reduced the need for fire suppression due to advances in fire prevention. Technology has provided the platform to make all this possible, but the world continues to become more complex, population areas are growing, and the threats to our safety and security are increasing.

The asymmetrical threat of terrorism and the occurrence of natural catastrophes in the last decade have punctuated the need for interoperability among agencies. For example, the terrorist attack on 9/11 caused the U.S. to re-evaluate how it performs coordinated response. The bombings in Madrid, London, and

Mumbai underscored the fact that terrorism is a global problem. In addition, Hurricane Katrina in the U.S., the tsunami in Thailand, and the wildfires in Australia demonstrated the need to expand response to “all hazards” for emergency management and interoperability. Security experts are expending considerable effort to improve preparation, prevention, detection, assessment, response, and recovery – moving us from a security paradigm of concrete and barbed wire to one of intelligence fusion. However, the challenges are sometimes exacerbated by the very technology we use to help us advance toward that goal.

3. Interoperability Concepts

Convergence is a buzzword that indicates the blending of voice, data, and video onto a network-centric environment based on all information delivered using IP. The good news is that IP is the plumbing that enables us to achieve operational interoperability. As we continue to move away from coaxial cables, serial interfaces, and analog telecommunications – and convert to digital IP – our initial standards challenge is all but solved. Interoperability, as the Merriam-Webster online dictionary defines it, is the “ability of a system (as a weapons system) to work with or use the parts or equipment of another system.” Most of us have heard the phrase a “system of systems” used as a computer architecture for solving today’s challenges. That is a great high-level concept, but we need to drill down more to solve our interoperability challenges.

It was mentioned earlier that the plumbing was in place already to enable interoperability, but that was only step one. Standards are mentioned often in discussions of interoperability, but what is really meant by standards? To answer that question, let’s define a couple of concepts.

Syntactic Standard

The first concept is a syntactic standard. Standards in this arena deal with communications protocols and data formats. Much like an alphabet forms the basis for a written language, syntactic standards form the basis for interoperability. Examples of syntactic standards are Extensible Markup Language (XML) and Standard Query Language (SQL). These form a standard way to format and exchange data.

Semantic Standard

The second concept is a semantic standard. Having a way to write a language does not mean we can communicate; we still need a vocabulary and grammar. The same is true with data. We need a means to communicate common ideas so there is no ambiguity. Therefore, the alphabet needs a structured language, or in the IT domain, a common information exchange model. An example of that is the U.S. National Information Exchange Model (NIEM), discussed later in this paper. This provides a semantic context with which to share data to enable information flow.

As software and system providers produce applications and solutions using these concepts, interoperability will become easier. We have the plumbing with networks and IP, the syntactic standards with XML and SQL, and the semantic standards with NIEM. This is the technical piece, but we must also consider the human part of this equation. Policy, doctrine, and governance are required to support the sharing of information among disparate organizations. As we develop and deploy technology, we must consider the importance of developing the concept of operations to adequately and efficiently leverage this technology. It is also important to define and manage what information gets shared, under what conditions it is shared, and who is authorized to access it. This is a more challenging problem than the technology evolution itself.

4. Today's Emerging Standards

Let's look at some examples of how standards are brought to reality in today's world. In the domain of emergency management and the operational environment this represents, the digital map is the visualization tool that enables the display of complex data for decision support. Geospatial context truly supports the old adage that "a picture is worth a thousand words." We hear the terms "common operational picture" (COP) and "user-defined operational picture" (UDOP) used to portray the concept of sharing operational information across an enterprise among commanders and responders. The industry has accomplished considerable work during the past decades to drive geospatial standards. The Open Geospatial Consortium (OGC[®]) and the European Union Infrastructure for Spatial Information in Europe (INSPIRE) are driving spatial data standards within the industry to insure entities can share spatial data. Following is some information on these efforts and how Intergraph solutions support them.

4.1. OGC Standards

The OGC is an international standardization association that includes more than 300 organizations and uses an open consensus method to develop and implement standards for geospatial processes. OGC standards are quickly evolving and enabling the geospatial industry to seamlessly access, query, and process disparate data sources and sensor information. OGC works closely with the International Organization for Standardization (ISO) to promote the global adoption of consistent standards. Intergraph is a founding and principal member of the OGC and contributes to the development of standards and the promotion of open geospatial interoperability in its service solutions. Intergraph's long-standing support of OGC, coupled with our top membership level, affirms our strong commitment to open geospatial interoperability. Support for OGC standards is essential across all industries.

4.2. Spatial Data Infrastructure and INSPIRE

In order to provide quality services to citizens and communities, decision-makers must have access to shared information from disparate sources. Geographic information systems (GIS) and spatial data infrastructures (SDIs) help officials take competent steps at local, regional, and federal levels in areas such as border security, emergency management, infrastructure management, land management, and public services. To ensure consistency, OGC standard support is essential.

SDIs are global and national directives and norms for data and service interoperability that layer on top of OGC and ISO standards. SDIs represent sets of agreed-upon rules, standards, and policies for seamless discovery, use, and processing of disparate geospatial data for governmental, commercial, and public purposes following the service-oriented architecture (SOA) paradigm. Various government initiatives have already defined their spatial infrastructure principles, including INSPIRE, United Nations SDI, Canadian Geospatial Data Infrastructure, and the National Spatial Data Infrastructure (NSDI) in the U.S. Intergraph has directly participated in INSPIRE since the spring of 2005, as well as on EU-funded projects related to INSPIRE. Projects include:

HUMBOLDT – Humboldt is an ongoing project for data harmonization and service integration. Intergraph brings to the project outstanding experience in the safety and security sector, combined with expertise in the SDI domain.

GIS4EU – The target of the project is to communicate which standards and INSPIRE-implemented rules are mandatory or optional, and the requirements for users and data providers toward harmonized geoinformation in Europe.

Image 2006 – This project aims to manage a common set of ortho-rectified satellite images and the related mosaic, including all collected images. These sets of data must be accessed and

disseminated according to the standards defined by the INSPIRE directive. Intergraph has performed a feasibility study, integrating its TerraShare® product suite into the IT infrastructure of the SDI unit of the Joint Research Center of EU (JRC) to manage and distribute Image 2006 datasets.

Intergraph's active participation in several organizations and initiatives that develop standards led to the expertise that allows us to empower our customers with the best SDI-enabled software. Intergraph's SDI application is built on top of Intergraph's GeoMedia® technology and will be enhanced by "SDI Pro" and "SDI Portal." Together, these offerings embrace all necessary services, structures, and user interface elements. More detailed information about SDI can be found in a separate white paper, "Providing Government Collaboration and Public Distribution with Spatial Data Infrastructures."

4.3 The IJIS Institute and NIEM

Several initiatives and groups strive to enable the sharing of information among organizations in the U.S. One organization that is steering the way for interoperability standards is the Integrated Justice and Information Systems Institute (IJIS). Here is a short description of IJIS from its Web site at <http://www.ijis.org/>.

"The IJIS Institute, a 501(c)(3) non-profit corporation, represents industry's leading companies who collaborate with local, state, tribal, and federal agencies to provide technical assistance, training, and support services for information exchange and technology initiatives. Serving as the voice of industry, we unite the private and public sectors to improve mission-critical information-sharing for those who protect and serve our communities.

The IJIS Institute was founded in 2001 as a result of the U.S. Department of Justice's interest in raising private sector participation in the advancement of national initiatives affecting justice and public safety, and more recently, homeland security. Today, the IJIS Institute represents the leading companies serving these and other related sectors. The IJIS Institute provides assistance to government agencies by bringing industry to the table in a constructive role, and continuing to drive toward achieving high regard for the companies that are dedicated to helping the public sector find high-value solutions. The IJIS Institute is funded through a combination of federal grants, industry contributions, and partnership agreements."

IJIS is helping to drive the adoption of NIEM, a semantic standard mentioned earlier, across the U.S. and even globally. Following is a brief description of NIEM from its Web site at www.niem.gov/.

"NIEM, the National Information Exchange Model, is a partnership of the U.S. Department of Justice and the Department of Homeland Security. It is designed to develop, disseminate, and support enterprisewide information-exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation.

NIEM enables information-sharing, focusing on information exchanged among organizations as part of their current or intended business practices. The NIEM exchange development methodology results in a common semantic understanding among participating organizations and data formatted in a semantically consistent manner. NIEM will standardize content (actual data exchange standards), provide tools, and managed processes.

NIEM builds on the demonstrated success of the Global Justice XML Data Model. Stakeholders from relevant communities work together to define critical exchanges, leveraging the successful work of the GJXDM."

To illustrate how IJIS and NIEM are being incorporated as standards in operational usage, we will look at a recent initiative driven by the City of Richmond, Virginia. One of the challenges related to security is the passing of alarm calls from a central station monitoring company to a public safety answering point

(PSAP). Typically this is accomplished by a phone call between the alarm company and the PSAP, which costs precious time and is prone to errors. Richmond began working to solve this issue by spearheading an effort to automate this process and develop a standard for the industry. The standard was approved in January of 2009.

Richmond's two-year pilot External Alarm Interface Exchange project, funded by the Department of Justice, Bureau of Justice Assistance, eliminated approximately 6,000 telephone calls from residential and commercial security companies. This reduction means more efficient use of 9-1-1 call-taker resources in the PSAP. Richmond uses the Intergraph Computer-Aided Dispatch (I/CAD) system, and together, Richmond and Intergraph worked to define, develop, and test the standard. The program's success has made it an American National Standards Institute (ANSI) standard now recognized by the Association of Public Safety Communications Officials International (APCO) and the Central Station Alarm Association (CSAA). Each year across the United States, 9-1-1 call-takers, managing more than 32 million incoming calls for assistance from alarm monitoring companies, stand to benefit from this standard.

By using an XML-based approach that conforms to NIEM to facilitate the electronic transmission of critical data from alarm monitoring companies to PSAPs, 9-1-1 call takers' time is no longer needed to manually gather and input alarm alert information. Instead, the computer-aided dispatch (CAD) system processes the new alarm event data as a call-for-service that appears instantly in the radio operator's dispatch queue for assignment to first responders. This automation has reduced response times by at least two to three minutes, saving precious time and lives.

IJIS awarded The City of Richmond and Intergraph the IJIS Institute Innovation Award for the Advancement of Public Safety in August 2009. The IJIS Institute Innovation Award recognizes technical achievements in public safety, justice, and homeland security that have contributed to the advancement of integration and interoperability.

To illustrate the importance of the standard, here are some quotes attributed to this initiative:

"It has been a special honor for the City of Richmond to have pioneered a technology project that has resulted in a new American national standard. The new ANSI standard can be deployed easily by all CAD and central station alarm monitoring software providers on behalf of 9-1-1 PSAPs and alarm monitoring companies. The collaborative and cooperative success of this interoperability project will reduce telephone call volumes between 9-1-1 PSAPs and alarm monitoring companies in the millions, reduce mistakes in the processing of new alarm events, and save lives and property. I am very pleased with Intergraph's role to become the first commercial CAD provider to complete this interface that conforms 100 percent to the ANSI standard." - Bill Hobgood, Public Safety Team Project Manager, City of Richmond, Virginia, Department of Information Technology

"APCO International applauds the City of Richmond and Intergraph for their focus on the end-users and the improved dispatch and response times gained through this project. This standard is highly recommended for all entities and agencies interested in implementing an automated exchange of alarm-related data in order to promote more efficient and effective public safety and data interoperability, as demonstrated in Richmond." - George S. Rice, Jr., Executive Director, APCO International

"Interoperability continues to be one of the most strategic imperatives in public safety. The automation of alarm alerts between the commercial and public sectors is an important new interoperability milestone." - Jeff Vining, Vice President and Research Analyst for Government, Homeland Security, and Law Enforcement, Gartner, Inc.

5. Beyond Map Data and the Support of a Sensor Network

A sensor network is a collection of spatially distributed sensing devices that can work together to collect and monitor data about particular phenomenon, such as environmental, telemetric, or motion information. The sensor network is by definition a heterogeneous, distributed, and loosely coupled set of sensor appliance capabilities that can effectively use the SOA approach in their operations.

The OGC Sensor Web Enablement (SWE) initiative defines a framework of open standards for using Web-accessible sensors, sensor systems, or sensor networks, which play a large part in safety operations. These specifications include, for example, standards for how to:

- Fetch observations or information from sensors – Sensor Observation Service (SOS)
- Perform command and control of the sensor – Sensor Planning Service (SPS)
- Publish/subscribe to defined alerts from the sensors – Sensor Alert Service (SAS)
- Communicate among SPS, SAS, and a client – Web Notification Service (WNS)

Intergraph is moving toward the adoption of these standards, as they will contribute to simplified integration within the public safety and security sectors. This implementation will enable customers in these industries to more easily link applications together and exchange data. Near real-time collection and analysis of information from heterogeneous sensor nodes, together with appropriate scientific models, chronological data intelligence, and user knowledge, can bring unparalleled value for just-in-time decisions and real-time organizational adjustment to changing conditions. Intergraph's support of OGC standards, our use of the SOA approach, and vast industry knowledge, combined with our offerings in sensor networks and alarms, guarantee our customers the most comprehensive and effective sensor-enabled solutions.

6. A European Program: Emergency Support System

Intergraph is a member of the Emergency Support System (ESS) Consortium approved by the European Commission to begin research and development of a portable emergency command-and-control system that incorporates real-time data collection technologies. The system will provide actionable intelligence to managers during crisis events and will provide a framework for future crisis management systems.

ESS will leverage Intergraph's extensive public safety and security expertise to develop the core of the ESS portal, the Data Fusion Mediation System (DFMS), which will collect data from different data sources and harmonize them into one comprehensive dataset. This dataset will then provide input to the Web-based ESS portal to help support decision-making in crisis situations. Intergraph will also have a significant role in the development of all work packages of the ESS project.

Part of the Seventh EU Framework Program, ESS is a four-year project expected to run until 2013. The European Commission will contribute €9.1 million over the next four years. The ESS consortium, which is led by Verint Systems, is composed of 19 leading European technology companies, research institutes, and end-user organizations.

The purpose of ESS is to improve control and management of major crisis events, such as terror attacks, industrial accidents, and natural disasters. The idea guiding the development of ESS is real-time fusion of various forms of field-derived data, including video, audio, weather, location tracking, radioactivity, biochemical, telecom derived data, affected population reports, and other information. The data will be communicated via both portable and fixed platforms, including wireless communication devices, unmanned aerial vehicles (UAVs), air-balloon, and field-vehicles. Fusion of the data occurs within a central system, which performs information analysis and provides decision-support applications for Web-based command-and-control systems. This provides flexible, yet comprehensive, coverage of the affected area.

Once available to the market, the ESS concept would offer real-time synchronization and information-sharing between first responders and support forces at the site of the incident. These include response professionals such as police, rescue teams, and firefighters, as well as out-of-theater command-and-control centers of the various involved authorities (e.g. municipalities and homeland security). ESS will also enable the commanders to communicate with affected on-site personnel by sending text (SMS) or recorded voice messages.

7. DHS Unified Command and Decision Support *

A new Department of Homeland Security (DHS) project called Unified Incident Command and Decision Support (UICDS) is delivering on the promise of information-sharing for emergency operations.

Acting Under Secretary of the Science and Technology Directorate, Bradley I. Buswell, testified before the House Committee on Appropriations, Subcommittee on Homeland Security, calling UICDS “a blueprint for managing and sharing incident information across state and local jurisdictional lines, and with DHS and other federal agencies.” Buswell said, “This national architecture, a response to issues identified in the 9/11 Commission Report, is aimed at establishing a set of standards to which solution developers for incident management tools will adhere in order to ensure that recipients of DHS funds at the state/local level will procure incident information management systems that comply with uniform standards in order to solve the information interoperability problems.”

By creating national “middleware” designed to support the National Response Framework and the National Incident Management System, including the Incident Command System, DHS is not imposing new requirements on governments. Rather, the standards are developed to create market opportunities for commercial, academic, volunteer, and government technology providers of incident management software and hardware. Thus, the goal is for technology providers to adapt their products to integrate with UICDS, while UICDS helps to expand the marketplace for incident management technologies. Everyone benefits and governments receive the next version of their chosen applications ready-made for information-sharing through UICDS.

UICDS for Government: No New End-User Software, No New Training

As middleware, UICDS does not interface directly with end-users. Rather, it relies on regular, daily use, external applications as the source of and visualization for relevant data. UICDS is the transporter of uniform data in common formats. External applications (sensors, incident logs, personnel management, dispatch systems, video surveillance, and intelligence tools – anything related to homeland security) provide a portion of their data to UICDS, which then publishes it to subscribers’ external applications. External applications then visualize the consumed data inside their own user interfaces. Thus, to the government end-user, there is no new application, no new learning, and no conscious sending of information.

Government users then become part of a decentralized network of, perhaps, thousands of UICDS cores with capabilities matched to end-user needs. For example, a large city, state, or multi-jurisdictional region’s UICDS installation may be a network of UICDS core servers fully integrated with CAD, traffic sensors, hospital admissions systems, public works equipment maintenance records, arrest and warrant management systems, weather sensors, and more. Scale down UICDS to a single computer, lower communication bandwidth, add fewer external applications, and UICDS serves any type or size of community – urban or rural, coastal or desert, ski resort or football stadium, multi-agency and multi-jurisdictional. Scale down UICDS even further, and it delivers critical information to a personal digital assistant (PDA) or a smart cellular phone – even to a radio through digital voice.

To the government user, however, all this happens in the background. The dispatcher does not change what he or she does. The resource manager, planner, and incident commander do not change the daily-use application they have chosen. Rather, the application adds a UICDS “adapter” that enables the government user to provide incident data to UICDS and other connected applications, and consume data from UICDS and other connected applications. UICDS can support all emergency operations, from everyday dispatches to major national emergencies.

*Source for UICDS information: www.uicds.us/files/UICDS%20in%20Brief%20Gov.pdf

7.1 UICDS Technology Providers*

In September 2008, the UICDS team held its first technology provider meeting to overview the objectives, benefits, and designs for UICDS. More than 125 representatives from companies, universities, and government participated in person in McLean, Virginia, and on the phone. Throughout the fall, the group held a series of special-focus meetings clustered around types of technologies and the UICDS services that support information-sharing. These included incident management technologies, geospatial applications, sensors, planning, and resource management tools. At these meetings, the objective was to harmonize the UICDS designs with the standards, data formats, and interfaces of current technology products. The UICDS goal was to launch UICDS with maximum input from technology providers and maximum use of existing interface standards and information-sharing methods.

Beginning in the spring of 2009, the group held biweekly technology provider conference calls to keep a focus on UICDS growth and share developments. On April 29, technology providers came together in Richmond, Virginia, to demonstrate their achievements in integrating through UICDS. Prior to UICDS, virtually none of the applications had an installation to share information with another. Yet, through the cooperative development process and the demonstration, all 23 were sharing information with at least one other entirely new application.

Through the remainder of 2009, the Virginia Division of Emergency Management will pilot UICDS in conjunction with several county and local jurisdictions. The focus of information-sharing will be on CAD, with additional applications to include GIS, sensors, traffic cameras, incident management applications, resource management, and other areas of interest.

Talk to any of the current UICDS participants and you will hear the story of consultation, collaboration, and inclusion as UICDS continues to improve its ability to meet the needs of the emergency management community. For government users, this means an ever-increasing number of technology providers complying with the UICDS interface standards.

To become involved in UICDS – and to help define the information-sharing you need, determine whether the applications you use today are becoming UICDS-conformant, and become an early adopter of the UICDS middleware for your community – e-mail the UICDS Technology Provider Outreach Director, James W. Morentz, Ph.D., at morentzi@saic.com.

*Source for UICDS information: www.uicds.us/files/UICDS%20in%20Brief%20Gov.pdf

8. Conclusion

To achieve operational interoperability in today's world is a complex endeavor. Standards are required to enable the sharing of data in both a syntactic and semantic context. Standards then enable systems to begin exchanging data and commands to derive information for decision-making and coordinated response efforts. To truly achieve operational interoperability, however, these standards must be put to the test. Government entities around the world are funding pilots to work through policy, doctrine, governance, and technology issues to drive these standards and approaches forward into the 21st century. A lot has been done and much is in place, but there is still more to do before applications and solutions are truly plug-and-play, and we achieve the desired state of complete operational interoperability.

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

Intergraph the Intergraph logo, TerraShare, and GeoMedia are registered trademarks of Intergraph Corporation. Other brands and product names are trademarks of their respective owners. Intergraph believes that the information in this publication is accurate as of its publication date. Such information is subject to change without notice. Intergraph is not responsible for inadvertent errors. ©2009 Intergraph Corporation. All Rights Reserved. 11/09 SGI-US-0005A-ENG