Smarter Cities Series: Understanding the IBM Approach to Public Safety

Redguides
for Business Leaders

Dr. Anand Paul
Mark Cleverley
William Kerr
Frank Marzolini
Mike Reade
Stephen Russo

- See how IBM Crime Prediction and Prevention and IBM Smart Vision Suite support public safety

- See how predictive analytics help turn data into actionable information

- Learn about turning digital video into information and intelligence

Redbooks

Introduction

A fundamental responsibility of public safety officials is to ensure the safety of its citizens and to protect assets. Many city leaders and public safety officials are investing in and applying new technologies and innovative approaches to reduce urban crime and improve emergency response. Since the 1930s, IBM® has been helping equip law enforcement officials around the world with information technology (IT) to help fight crime faster, more safely and more effectively. Today, public safety challenges continue to increase in known and previously unforeseen ways.[1]

New technologies and capabilities are available to help improve public safety systems, enhancing connectivity, improving efficiency and making them smarter. Instead of just reacting to crimes and emergencies, with these new technologies and capabilities, public safety officials can perform analysis so that they can anticipate and work to prevent incidents. These smarter public safety systems can collect data from different processes, systems, and devices and can apply intelligence to this mass of data. The intelligence applied to this data can detect patterns of incidents and generate new insights, so that officials can make well-informed decisions and take action in near real time.

IBM has been working with various city and national agencies around the world applying technology and capabilities to avert crime and help resolve criminal acts effectively. Cities understand that citizens decide where they live, work and play based partly on their sense of safety. Public safety solutions from IBM can help public safety officials address crime by giving them the ability to respond in more proactive and effective ways when situations arise.

This IBM Redguide™ publication highlights the IBM approach to creating a smarter public safety environment. It provides a high-level overview of two key solutions:

► The *IBM Crime Prediction and Prevention solution* helps law enforcement agencies develop a more responsive, dynamic and optimized police force that can increase community safety and improve the effective and efficient use of agency resources. This solution includes IBM analytics tools and data management techniques to help law enforcement agencies improve their results in policing, crime analysis, performance and decision making.

► The *IBM Smart Vision Suite* is event- and search-based video analytics technology that can be used to detect unusual patterns of activity in a defined area. For example, this solution can be used to alert security personnel to a possible security breach or threat in a train station, in and around buildings, or in an airport environment.

---

[1] IBM 100, Predictive Crime Fighting: http://www.ibm.com/ibm100/us/en/icons/crimefighting/

1

This guide concludes with a sampling of cases studies from engagements that IBM has conducted with various law enforcement agencies.

To understand the broader picture of IBM Smarter Cities®, see the following Redguide publications:

► *Smarter Cities Series: A Foundation for Understanding IBM Smarter Cities*, REDP-4733

► *Smarter Cities Series: Introducing the IBM City Operations and Management Solution*, REDP-4734

Approach to Smarter Public Safety

The IBM approach to Smarter Public Safety® is through investment in reusable and open standards-based technologies that enable improved information and intelligence sharing among private and public safety agencies. Through improved planning, system integration and collaboration, public service providers can better protect citizens while lowering the risk of loss to public and private infrastructure.

The IBM Smarter Public Safety approach enhances preparedness and situational awareness. It also enables a more effective response through the smarter use of resources. This approach further suggests investment in information sharing and analytics to extract greater insight and value from existing information repository investments. The application of analytic tools and information sharing provides public safety agencies with the insight and intelligence required to prevent or reduce the risk of public safety issues.

The IBM Smarter Public Safety solutions optimize the use of public safety personnel, resources and technologies in protecting citizens and assets. This guide addresses the following IBM Smarter Public Safety solutions:

► IBM Crime Prediction and Prevention solution
► IBM Smart Vision Suite

The combined technology of IBM and i2: On 31 August 2011, IBM announced the acquisition of i2 to accelerate its business analytics initiatives and to help clients in public safety address crime, fraud and security threats. This acquisition extends IBM leadership in helping clients harness their "big data" that consists of massive amounts of information. This data also consists of intelligence coming from disparate and unstructured sources including social media, biometrics and criminal databases. With the addition of i2 intelligence analytics for crime and fraud detection capabilities, IBM can help cities, nations, and international bodies combat fraud and security threats.

With IBM and i2, clients have access to a comprehensive range of visualization and multidimensional analytics for the timely delivery of intelligence, including threat and fraud analytics. For more information about this announcement, see "IBM to Acquire i2 to Accelerate Big Data Analytics to Transform Global Cities" at:

http://www.ibm.com/press/us/en/pressrelease/35255.wss

For more information about i2, see the i2 website at:

http://www.i2group.com/us

IBM Crime Prediction and Prevention solution

Law enforcement organizations understand that the data they have already collected is an invaluable source of information for carrying out investigations. However, like many other organizations, significant challenges arise when data is not shared across departments or organizations, leading to inefficient use of the available information.

Law enforcement worldwide face some of the following more common challenges, among others:

► Investigators and detectives face heavy caseloads. They need the right information at the right time to make decisions and to better manage cases.

► Officers need actionable alerts and reports delivered in an effective manner to determine an appropriate response, streamline the arrest process and provide for their own safety.

► Investigators need a better understanding of the individual identity and relationships of perpetrators, suspects and victims for which information is frequently lacking.

► Police commanders need summary and historical information to evaluate tactical effectiveness and outcomes.

► Police commanders need the ability to dynamically reallocate forces to defeat a pattern of crime or position officers to prevent expected criminal activity.

► Law enforcement needs the ability to identify a pattern of criminal activity, cutting the time to make an arrest.

► Law enforcement needs the ability to predict criminal activity, reducing the risks to citizens and officers.

The following challenges are the basis for law enforcement organization requirements:

► Obtain a holistic view of perpetrators, suspects and victims from non-obvious relationships hidden in data systems.

► Integrate information from various sources such as national, provincial, state and local agencies.

► Perform perpetrator or suspect status tracking.

► Generate actionable alerts to pre-empt criminal activity and safety risks.

► Meet local, regional and national requirements for reporting processes, such as Uniform Crime Reporting (UCR) and National Incident Based Reporting System (NIBRS) in the US, and support accountability processes such as CompStat.

► Support a flexible and robust reporting environment that includes ad hoc and exception reporting.

► Provide predictive capability to detect, define and deter criminal activities.

Solution overview

To help law enforcement agencies improve public safety and security, IBM has identified the following key goals:

► Sense, respond to, and resolve incidents in an efficient and effective manner.

Improving criminal identification and investigation using complete identification of persons of interest, perpetrators, suspects and victims gives officials a better understanding of the persons involved. Other important capabilities to use in incident handling are visualization of criminal and location information, and analysis of criminal history of suspects.

► Collaborate and share information to improve outcomes.

Collaborating and sharing data and information with other agencies and organizations can improve outcomes, by having access to critical information about an incident or investigation.

► Predict patterns and threats to prevent crime.

Analytic tools applied to trusted data can be used to perform crime prediction, develop criminal pattern definition, and aid in crime prevention. Analysis results can be used to establish adaptive, effective force deployment and evaluate command performance.

► Improve effectiveness of citizen services and business operations.

Safety and security can be improved by applying IBM technology, such as in the following ways:

► Integrate and deliver data to enable better decision making, to support investigations and improve officer safety (by aggregating data sources to help identify individuals and their networks), to analyze crime patterns and to measure program performance.

► Provide insight into data to support command decisions, enabling the redeployment of resources in response to crime patterns and trends.

► Use predictive analytics to identify the potential for criminal activity, which can occur based on historical crime data, other influencing factors and trigger events.

The Crime Prediction and Prevention solution assists law enforcement agencies with data integration to gain a holistic view of the persons, objects, locations and events (POLE). This solution helps in conducting investigations, implementing accountability programs to improve police performance, and defining and identifying criminal or threat-related patterns.

Figure 1 provides a conceptual overview of the Crime Prediction and Prevention solution.

Flexible deployment: The IBM Crime Prediction and Prevention solution consists of a suite of products and capabilities that can be deployed individually or in combination to meet the specific requirements of an agency.
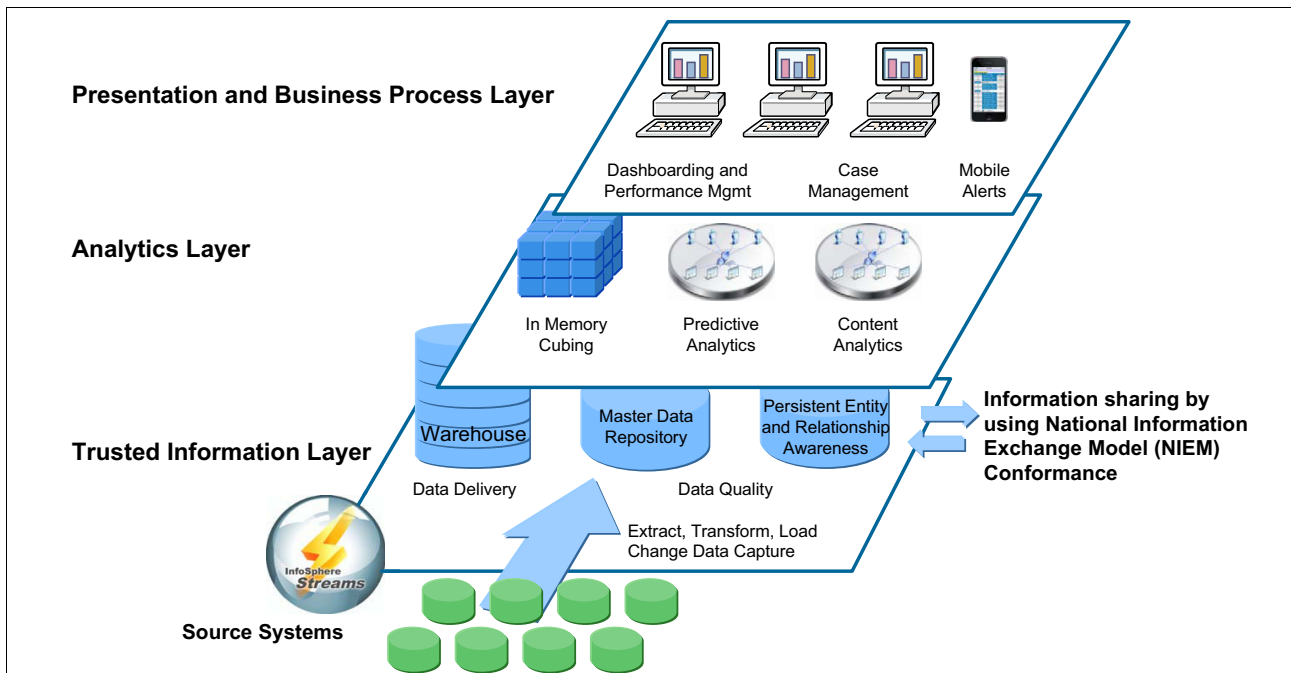

Figure 1   Crime Prediction and Prevention conceptual overview

Figure 1 on page 4 shows the following components:

► Existing systems and environments provide input into the solution:

– Source systems including the following components:

• Internal systems, such as Computer Aided Dispatch (CAD), Records Management (RMS) and ancillary functional databases

• External data, such as watch lists, intelligence reports, corrections, parole and probation records

– Structured and unstructured data, such as email, social media content, 9-1-1 call transcripts, case narratives and field reports

– Data that might be shared bidirectionally with external agencies, other jurisdictions and within the organization

Information sharing is best accomplished using industry standards. For example, the US uses the National Information Exchange Model (NIEM). This model is an XML-based data framework for information exchange across many levels of public safety agencies. NIEM is being considered for adoption across many government domains and by other countries that collaborate with the US.

► The Crime Prediction and Prevention solution consists of these the following capabilities:

– The *trusted information layer* collects, manages, shares and delivers information that is accurate, complete and in context, which helps to provide a more insightful view of the data or information to the system users. The IBM Crime Information Warehouse from IBM Global Business Services® provides a proven approach to delivering the trusted information layer. For more information about IBM Crime Information Warehouse, see "Delivering trusted information with IBM Crime Information Warehouse" on page 7.

The following key capabilities are necessary for handling, storing and retrieving data:

• The *extract, transform and load (ETL) process* supports the collection, cleansing, transformation and integration of large volumes of data and supports simple to highly complex data structures. Issues with data quality are addressed by using proven tools and methods. Change data capture enables near real-time updates to data that occur during transactions in the applications from any source system.

• *Data warehouses* are a repository for all types of data that are used for reporting and analysis.

• The *Master Data Repository* manages and maintains master data for multiple systems and processes. It delivers a unified, complete, consistent, and standardized view of key entities, such as persons of interest, incidents and events, objects and locations.

• *Persistent entity and relationship awareness* is a unique capability that establishes a trusted view into an identity. It supports identity discovery and analysis through culturally aware name standardization and matching and through non-obvious relationship awareness. This capability can help law enforcement to accurately identify suspects and victims and to identify non-obvious relationships between people and other POLE elements.

Entity and relationship awareness has a persistent context that acts in near real time to allow new information to correct earlier assertions. In turn, this approach enables all interactions with the system (such as queries, transactional data or new data source loads) to continuously resolve and correct entity records and their hidden relationships. This activity occurs simultaneously with providing notifications based on new threat information as it is identified.

Persistent entity and relationship awareness provides results that can more quickly identify potential suspects and known whereabouts and that can identify linkages

between POLE elements to several degrees of separation. These results can be delivered in many formats, including Identity Resume, which provides a complete, holistic view of an individual in a single document. The results can also be viewed by using the Visualizer tool that shows the relationships between POLE elements in an interactive diagram. Also, the results can be exported into various visualization and presentation products through a web services interface.

– *Analytics layer* harnesses various business intelligence and analytics tools that are used to analyze data stored in the trusted information layer.

- Query, reporting and analysis provide the capabilities to dynamically create, view, assemble and analyze all the pertinent data to a situation. Querying data and generating reports (which can be shared and further analyzed) provide the necessary information required to take action and make well-informed decisions.

- Content analytics provides capabilities to access, aggregate, analyze and visually explore large volumes of unstructured content. It helps to identify trends, patterns and deviations, improving management decisions and optimizing processes. With content analytics, departments can uncover insights in complex data (such as documents and narratives, audio recordings, video clips, or web content, including social media) in near real time. This type of analysis can take days, weeks or longer to accomplish when done manually.

- Predictive analytics helps connect data to effective action by drawing reliable conclusions about current conditions and potential future events. The application of predictive analytics to data helps uncover unexpected patterns and associations to guide awareness and actions. By using the results of this analysis, organizations can anticipate events and act proactively, preventing or minimizing incidents and improving outcomes.

  For example, by combining multiple data sources, predictive analytics can help predict the conditions and circumstances where crimes are likely to occur. It can produce models that are used to help understand criminal patterns, identify behaviors as part of a criminal pattern or trend, and predict the incidence of criminal activity. The models generated are based on proven statistical and historical analysis of data. These capabilities are central to establishing predictive policing programs. For more information, see "Predictive policing with predictive analytics" on page 8.

– *Presentation and business process layer* provides the access point to information and processes. How and when information is delivered and to whom it is delivered are of critical importance in the successful deployment of the Crime Prediction and Prevention solution. The presentation and business process layer can contain the following information:

- With dashboard capabilities, users can assemble and personalize their view of information to support their decision-making approach. With this view, the user can bring all related information together for a comprehensive view.

- Performance Management provides management with the visibility and information needed to ensure service quality and to reduce operations costs. For example, Performance Management can monitor various activities, such as responses to 9-1-1 calls and criminal identification and apprehension.

- Advanced case management unifies information, processes and people to provide a 360-degree view of the case. With advanced case management, skilled users can extract critical case details using integrated business rules, collaboration and analytics. All of these capabilities enhance their decision making abilities and lead to more successful case outcomes.

- Mobile reporting and alerts deliver the most critical information and analytic capabilities where they are needed in the field. Also this mobilization of information and capabilities enhance situational awareness, improve officer and public safety, and support conducting investigations at the scene of a crime.

Governance, security and monitoring capabilities are essential to protecting information and the operating environment. Governance establishes sustainable management of information integrity, availability and quality across its complete life cycle. Governance also ensures that proper audit trails are established. Security ensures that proper access to information, data, and systems is given to individuals and other systems. Also, security protects against cyber attacks, malware and other potential security breaches. Monitoring ensures that information remains protected by auditing users, assessing vulnerabilities, and validating compliance with regulations and policies.

Delivering trusted information with IBM Crime Information Warehouse

The IBM Crime Information Warehouse provides law enforcement agencies and police departments the ability to integrate data to better understand criminal patterns. It enables near real-time reporting, analysis and understanding of crime statistics. It also provides instant access to timely and accurate information so that departments can redeploy forces in response to crime trends as they occur rather than after they occur.

This solution provides the following features:

► A single, integrated, and coordinated repository for crime information data that is in compliance with government standards and police department initiatives

► An easy-to-use interface so that users can access and share information, reports and analysis results

► Standard reports and ad hoc queries so that law enforcement officials can gather the information they need to make well-informed decisions

► Investigative analysis tools to help in solving crimes and to enable better resource deployment strategies

The Crime Information Warehouse provides components that deliver statistical and analytical reporting capability regarding criminal information. It serves as the foundation for holistic determination of POLE. It is a single, integrated and coordinated source of crime information data that is validated in accordance with federal and state reporting standards and police department initiatives.

The IBM Crime Information Warehouse provides investigators and officers with current information about offenses and criminals so that they can solve criminal cases faster. Also, the Crime Information Warehouse contains historical data used by law enforcement analysts to model and identify crime patterns so that preventive measures can be implemented.

The Crime Information Warehouse provides the following advantages:

► Links day-to-day operations with criminal investigations, crime analysis, officer alerting and crime prediction

► Provides visibility into, and visualization of, holistic identity and historical criminal activity

► Provides a key tool for command structures to make informed decisions about the management of law enforcement activities

The IBM Crime Information Warehouse integrates existing data from disparate sources into a consistent, accurate information structure. The results are better use of existing information, which can improve officer safety and reduce crime on the streets, both of which are important to proactive policing.

Predictive policing with predictive analytics

Predictive policing approaches are being evaluated in many cities and have proven to reduce crime levels by preventing, rather than just responding, to criminal activity. Predictive analytics software enables predictive policing strategies. Predictive policing is accomplished by applying sophisticated statistical analysis, data mining and machine-learning techniques to historical crime and other relevant data to uncover hidden patterns and trends. It draws on data from sources that are inside and external to law enforcement agencies, collecting data that has value in predicting threats, behaviors and events. The data includes factors that can influence or trigger criminal activity, such as public events, weather, business type and location, and other geographical features. This data often resides in large files and in textual formats, such as narratives, email, and social media. By applying predictive analytics to this diverse data, agencies can anticipate events and identify the types of intervention needed and where it is needed.

Predictive analytics can be used to identify relatively subtle differences in behaviors that other methods often miss. For example, with predictive modeling, analysts can combine their knowledge, first-hand experience and intuition with the data and then guide the application of various analytical techniques. The ability to combine various data dimensions, types and sources on an ongoing basis makes it possible to quickly and reliably detect patterns, conduct investigations more efficiently and recognize hidden threats.

Today, predictive analytics is used in several justice and public safety domains. For example, in offender management situations, predictive models exist to predict behaviors and intervention outcomes, resulting in more effective offender rehabilitation and measurable reductions in recidivism. Also, several law enforcement agencies have employed predictive analysis to deploy resources effectively in areas and times where crime is most likely to occur.

Predictive analytics can include the following other candidate applications:

► Aiding investigations by identifying potential suspects based on previous behaviors modeled with the specifics of the crime
► Helping in risk analysis related to border security and immigration
► Preempting insider threats
► Identifying fraud and money laundering schemes and activity

IBM predictive analytics software is a comprehensive, easy-to-use set of statistical and predictive analytics, reporting, and decision support tools. These products can help law enforcement agencies move away from operating in a *sense and respond* mode and move to a *predict and act* mode.

Standards

The following standards are emerging to support law enforcement and public safety:

► National Information Exchange Model connects agencies so that they can collaborate and develop innovative, data-driven, mission-focused solutions. It develops, disseminates, and supports enterprise-wide information exchange standards and processes. With this approach, jurisdictions can effectively share critical information in emergency situations and support the day-to-day operations of agencies throughout the nation.

For more information about NIEM, see the NIEM website at:

https://www.niem.gov/

► Global Reference Architecture (GRA) is a reference architecture with guidance for identifying, defining, implementing, and governing services, enabling the integration of diverse systems. It is an information exchange solution that cuts implementation time and costs for state and local justice agencies through reuse of established and promising practices in IT architecture and design.

For more information about this specification, see the GRA web page at:

http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015

► US national standards for reporting of criminal activity include the following programs:

– Uniform Crime Reporting (UCR):

http://www.fbi.gov/about-us/cjis/ucr/ucr

– National Incident Based Reporting System (NIBRS):

http://www.icpsr.umich.edu/icpsrweb/NACJD/NIBRS/

IBM Smart Vision Suite

Situation awareness is the key to security. Awareness requires information that spans multiple scales of space and time.[2] Organizations are looking for ways to get more value from their physical awareness systems. A security analyst needs to perform the following tasks:

► Identity tracking: Who are the people and vehicles in a space?
► Location tracking: Where are the people in a space?
► Activity tracking: What are the people, vehicles or objects in a space doing?

A security analyst must also use a historical context to interpret this data. For example, the fact that the paper delivery truck arrived at 6:00 a.m. instead of the usual time of 8:00 a.m. might alert a security analyst to a problem.

Traditional physical awareness systems have many challenges, such as the following examples:

► Lack of effectiveness

– Inefficiency in "human eye" surveillance (Efficiency drops to 5% within 22 minutes.)
– Security is reactive, not proactive (A typical response is after an event has occurred.)
– Hardly ever used large amounts of video data
– No consolidated view of activity and security threats at the enterprise level
– Limited data sharing and integration between stakeholders
– Poor compliance and audit of approved security processes
– Lacking ability to mine data for patterns and vulnerabilities

---

[2] "Smart Video Surveillance Exploring the concept of multiscale spatiotemporal tracking," *IEEE Signal Processing Magazine* Volume 38, March 2005: http://www.research.ibm.com/peoplevision/IEEESP05.pdf

- ► Ongoing cost
  - – The staff to monitor closed-circuit television feeds
  - – The ability to retrieve, manage and store video content
  - – The need for proprietary hardware, maintenance and support

The amount of data is exploding, and its nature is changing to machine-generated data coming from devices such as sensors, cameras, radio-frequency identification (RFID) and Global Positioning System (GPS) systems. Cities face several security-related challenges:

- ► Scalability
  - – Cameras in high-traffic areas can generate hundreds of thousands of events each day.
  - – Hundreds of cameras in high-traffic areas can be deployed at the same time:
    - • Tens of millions of summarized events each day
    - • Hundreds of millions of trajectory events each day
- ► Application availability
  - – The system must operate 24x7, allowing for no downtime.
  - – Access to the informational data store must occur as new metadata is ingested.
  - – Relevant information must be easily and quickly accessible, regardless of the volume of incoming metadata.
  - – Application maintenance must occur while the application is still in operation.
- ► Content management
  - – The purging of aged data from the system must be done in a timely manner.
  - – The data purge process must not affect the addition of new or inbound metadata.
  - – The data purge process cannot affect online application availability.
- ► Fast access to informational data
  - – Indexing of specific categories of metadata is needed.
  - – Rapid response to event searches is needed.

Solution overview

IBM Smart Vision Suite is an open and extensible framework for event integration and correlation with search-based video analytics. It supports both advanced real-time alerts and highly specialized content-based search capabilities based on multiple object attributes. It provides event-based monitoring, analyzing video feeds in real time to provide instant alerts for the security staff.

IBM Smart Vision Suite includes the following capabilities:

- ► Search-based video indexing
- ► Real-time instant alerts
- ► Multi-sensory compound search on metadata
- ► Event cross-correlation from cameras and other sensors
- ► Integrated video management from partners
- ► Advanced event summarization and visualization
- ► Open framework for integrating sensors and events streams from other applications
- ► Advanced system management capabilities

Additionally, IBM Smart Vision Suite supports activity search, cross-correlation, and trend analysis for efficient review of video footage in both real-time and investigative circumstances. It can identify perimeter breaches, abandoned objects, objects removed, people, and vehicle

activity. The solution provides license plate and face recognition to maintain a history of the cars or people who enter the property and buildings of a facility.

The capabilities of Smart Vision Suite can complement and enhance an existing security infrastructure to provide defensive in-depth security on a continuous basis. This solution can be used in any industry and business environment. It indexes the video data streams to facilitate the retrieval, analysis, and correlation of events:

► Creates real-time alerts for events

► Provides extensive indexing and search criteria:

  – Attribute-based search (size, color, shape, moving, or non-moving)
  – Date stamp or time stamp, by camera
  – Post-incident review
  – By location in field of view
  – License plate search
  – Tracking path of object movement

► Offers customizable dynamic behavior analysis based on user-defined criteria or new threat models

► Reuses the same video feed for multiple applications (for example, people counting, loss prevention, and behavior monitoring)

► Integrates with existing cameras and network infrastructure

► Increases productivity and efficiency

High-level component overview

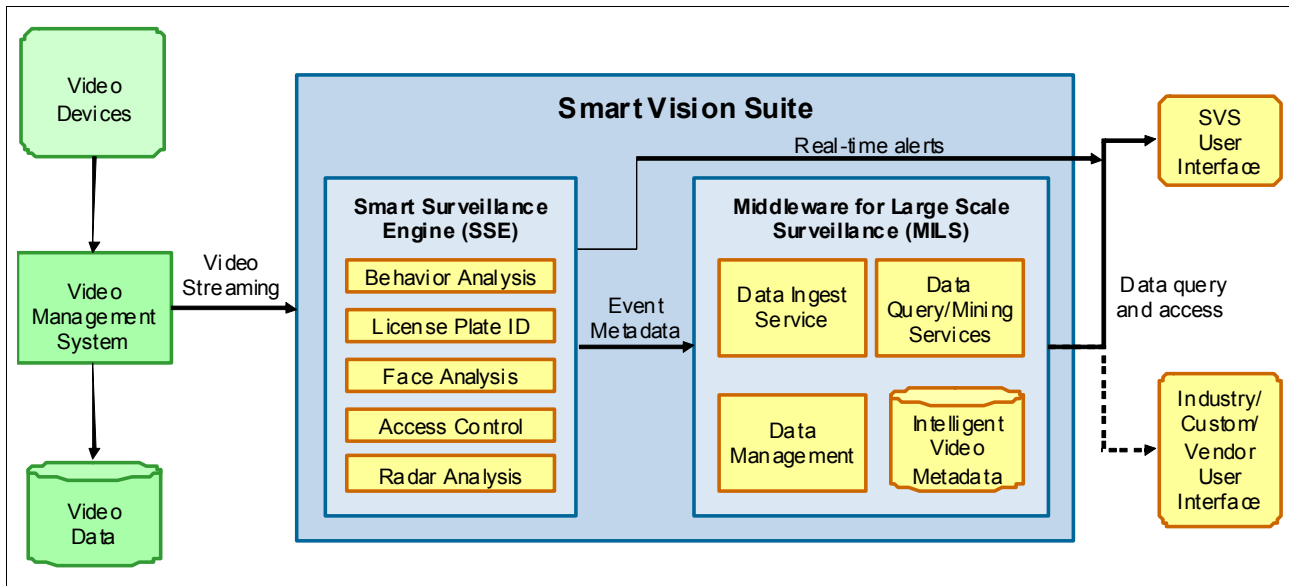Figure 2 provides a high-level component diagram of the Smart Vision Suite.

Figure 2   Smart Vision Suite high-level component overview

Figure 2 shows the following components from left to right:

► Video devices (including digital video, IP video cameras, networked video recorders, web video, consumer cameras, and video-based intelligence) provide video data on various objects such as parking lots, license plates and faces. The cameras can be deployed with a specific function in mind. For example, a camera can monitor a parking lot providing a

broad view, but a camera positioned near a door can capture the faces of people entering the facility.

► Video Management System consists of the hardware and software used to collect, store and retrieve video data from these devices. These systems are available from various partners that provide several solutions.

► Events are fed to the Smart Vision Suite, which consists of two main components:
  – Smart Surveillance Engine (SSE)
  – Middleware for Large Scale Surveillance (MILS)

  For more information about these components, see "Key components of Smart Vision Suite".

► Security personnel can receive alerts, view events and perform queries from the user interface provided by Smart Vision Suite or by industry, custom and vendor user interfaces.

Key components of Smart Vision Suite

The Smart Vision Suite consists of the following components:

Smart Surveillance Engine

Provides the front-end video analysis capabilities based on automatic image analysis technologies. Also provides alerts as needed.

Middleware for Large Scale Surveillance

Provides data and content management capabilities. Also integrates metadata from various analytics and indexes it into an *extensible* timeline data model. MILS relies on a database with tables that support various searches on the data.

Smart Surveillance Engine

SSE is a framework to capture real-time events that are observed by video devices, such as cameras. One SSE server can support multiple cameras. Each camera in the environment is assigned to an analytic engine running on an SSE server.

The specific user functionality that is associated with each camera is based on the profile, which is configured for use by the analytic engine associated with the camera. The analytic engines include the following capabilities:

► Behavioral analysis. Analyzes the movement of objects within the field of view of a camera, by detecting and tracking multiple moving objects across the camera, classifying these objects, and extracting various object attributes such as color, shape and size.

► Face analysis. Automatically detects images of human faces from the video. The face detection capability creates an index in the video and marks the time at which the face was present in the video.

► License plate recognition. Detects the presence of text within a given video frame, and then applies optical character recognition (OCR) technology to extract the license plate number.

SSE alerts are conditions that are specified by the user as being of interest. SSE supports basic video alerts and compound metadata-based alerts. The basic video alerts include the following capabilities:

Motion detection   Detects motion within a specified region of view.

Tripwire   Detects directional crossing of a user-defined tripwire.

Region   Detects behavior within a specified zone, such as entering, leaving, starting and stopping.

Abandoned object	Detects when an object is left behind.
Object removal	Detects when an object is taken away.
Directional movement	
	Detects when objects move in a user-specified direction.
Camera move/blind	Detects changes in camera state such as movement or obstruction.
Camera movement stop	
	Detects when a pan-tilt-zoom camera stops moving.

The SSE sends video metadata in XML format to the MILS central data repository and instructs it how to index the video.

Middleware for Large Scale Surveillance

MILS provides consolidated back-end data management capabilities and stores metadata that describes key activities that are discovered while ingesting video data. MILS can create and manage an index of the ingested video data, which has a full set of searchable event attributes to support forensic analysis. These attributes can also be used to define composite metadata-based alerts by combining the metadata in various ways to define complex behavioral patterns.

With IBM Smart Vision Suite, administrators can add new metadata schemas, enabling new analytic engines to send sensor and event metadata to MILS. The metadata from all analytic engines can then be cross-correlated, so that users can search across modalities. These advanced indexing capabilities offer a unique and powerful differentiator from virtually all other available solutions. In addition to metadata management, MILS provides system management, user management and various extensibility services, including a web services application programming interface.

For more information about Smart Vision Suite, see the following documents:

► *Smarter safety and security solution for rail: Deliver comprehensive video analytics with IBM Smart Vision Suite*

   `ftp://ftp.boulder.ibm.com/common/ssi/rep_sp/n/TTS03024USEN/TTS03024USEN.PDF`

► *S3-R1: The IBM Smart Surveillance System - Release 1*, by Arun Hampapur

   `http://www.research.ibm.com/peoplevision/IBMS3-R1Overview.pdf`

► *Digital Video Surveillance: enhancing physical security with analytic capabilities*, by Steve Russo, February 2008

   `http://www.ibm.com/services/us/gts/pdf/sp_wp_digital-video-surveillance.pdf`

Case studies

This section includes a sampling of IBM case studies that involve law enforcement agencies. For more Smarter Public Safety case studies, go to this web address:

`http://www.ibm.com/smarterplanet/us/en/public_safety/examples/index.html`

Memphis Police Department

Memphis Police Department (MPD) has enhanced its crime fighting techniques and has reduced serious crime with IBM predictive analytics software. MPD can now evaluate incident patterns throughout the city and forecast criminal *hot spots* to proactively allocate resources and deploy personnel, resulting in improved force effectiveness and increased public safety.

IBM predictive analytics software compiles volumes of crime records in seconds, including incoming data sources from patrols that pertain to the type of criminal offense, the time of day, the day of the week or various victim or offender characteristics. MPD can now better guide daily decisions that address criminal activity and place officers in a better strategic position to respond to an unfolding crime.

For more information about this case study, see "Memphis Police Department Reduces Crime Rates with IBM Predictive Analytics Software" at:

http://www.ibm.com/press/us/en/pressrelease/32169.wss

For additional information about the MPD case study, see these web addresses:

► Memphis PD: Keeping ahead of criminals by finding the "hot spots"

   http://www.ibm.com/smarterplanet/us/en/leadership/memphispd/assets/pdf/
   IBM_MemphisPD.pdf

► IBM Business Analytics SPSS: Memphis Police Department

   http://www.ibm.com/software/success/cssdb.nsf/CS/
   SSAO-8DJ5CL?OpenDocument&Site=default&cty=en_us

For a video of the MPD solution, go to the IBM Government industry page (under heading *Memphis PD: Fighting Crime with Analytics*) at:

http://www.ibm.com/services/us/gbs/industries/government/

Edmonton Police Department

Edmonton Police Service (Canada) is using IBM business analytics technology. With this technology, Edmonton police officers can view data in near real time. This technology makes crime information directly available to patrol officers so that they can use it to quickly identify problems, associated trends, and locations of crimes.

Edmonton Police Service uses business analytics to pinpoint crime trends and make quick decisions about resource deployment. As of September 2011, the police service has seen a 20 percent reduction in violent and property crime, resulting in over 4000 fewer victims of crime. This information helps police officers determine their response and identify problem-solving solutions. With this technology, police officers can monitor their performance strategically over time and place, and tactically on a day-by-day and call-by-call basis.

From more information about this case study, see "Edmonton Police Service Fights Crime with IBM Business Analytics Technology" at:

http://www.ibm.com/press/us/en/pressrelease/28455.wss

Summary

City and national public safety agencies are responsible for ensuring the safety of its citizens and protecting assets. Public officials are turning to the same technology advances that businesses use to make public safety systems smarter. Analytic technology and access to vital data will help public officials move from responding to events after they occur to anticipating and preventing events whenever possible.

The IBM Redguide highlighted the IBM approach to creating a smarter public safety environment. It provided a high-level overview of two key solutions: the IBM Crime Prediction and Prevention solution and the Smart Vision Suite. This guide concluded by highlighting cases studies from engagements IBM has conducted with various public safety agencies.

IBM can help public safety agencies make public safety systems smarter. IBM can also help drive a basic shift from responding to events to anticipating and minimizing the impact or even preventing them.

Other sources for more information

For additional information, see the following resources:

- Smarter Publics Safety web page

  http://www.ibm.com/smarterplanet/us/en/public_safety/ideas/index.html

- IBM Government industry page, which includes public safety

  http://www.ibm.com/services/us/gbs/industries/government/

- *Smarter Cities Series: Understanding the IBM Approach to Traffic Management*, REDP-4737

  http://www.redbooks.ibm.com/abstracts/redp4737.html

The team who wrote this guide

This guide was produced by a team of specialists from around the world working with the International Technical Support Organization (ITSO).

Dr. Anand Paul is the Research Relationship Manager for IBM Global Government Industry, and is with the IBM Research Division. He has more than 25 years of experience in developing Research strategy and implementing new technologies for clients. He has published more than 50 technical papers. Dr. Paul holds a Ph.D. in Materials Science and Engineering from The Pennsylvania State University and a Master of Business Administration degree from the University of Pittsburgh.

Mark Cleverley is Director of Strategy or IBM Global Government Industry, working with governments in many nations and many solution domains. He focuses on new technologies and their impact for government, most recently including smarter cities, social media, and cloud. He recently led the public safety element of IBM Smarter City summits. Previously, he was responsible for IBM Public Safety, Justice, and related clients in Europe, the Middle East, and Africa.

William Kerr is a senior certified IBM Consulting IT Architect and has been with IBM since 2000 working for IBM Global Business Services (GBS). With 33 years in IT, Bill has spent the

past four years selling and delivering to state and local governments in the northeast part of the US. He has led design, build, and deployment efforts for a New Jersey (NJ) state-wide Traffic Management Center, the NJ State Police Fusion Center solution in the IBM Waltham Interoperability Lab, and the NJ Tax fraud solution for the NJ Division of Taxation.

Frank Marzolini is the Global Solution leader for Government on the IBM Information Agenda® Tiger Team, specializing in law enforcement and threat prevention. Frank has been a Systems Integrator for over 25 years, with experience in the public sector, working with large-scale agencies in law enforcement, tax and revenue, and election agencies. Frank has worked with global, city, and state governments and agencies. He has been responsible for the construction of multiple large-scale systems.

Mike Reade is a Business Value Analyst on the IBM US Information Agenda team. He has over 23 years of experience in government Information Technology, specializing in law enforcement crime prediction and prevention and analytics for public safety. His areas of expertise include business and solution development initiatives and technology and services for cyber security, law enforcement, emergency management, intelligence analytics, and physical security. He has been an active member of the Integrated Justice Information Systems Institute and participates on the Emerging Technology Advisory committee. He is a frequent speaker at Public Safety conferences and has written extensively on IBM IT technology and solutions that support Public Safety.

Stephen Russo is the IBM Director of Security and Privacy Technology. For the past five years, he has been responsible for IBM Public Safety Physical Security technology, which includes an advanced set of computer vision analytics originally conceived and implemented by IBM Research. His current focus is on innovative solutions in physical security to move from passive "after-the-event" systems to proactive intuitive intelligence systems. Steve has 22 years of engineering and systems deployment experience. He was formally educated as an electrical engineer and computer science engineer at the University of Connecticut.

Thanks to the following people for their contributions to this project:

Michael Cosgrove
Business Development Project Manager, IBM Ireland

Dr. Gary Nestler
Global Public Safety, Subject Matter Lead, IBM US

LindaMay Patterson
IBM ITSO, Rochester, MN

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author - all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- ► Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- ► Follow us on twitter:

  http://twitter.com/ibmredbooks

- ► Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- ► Explore new IBM Redbooks® publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- ► Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document, REDP-4738-00, was created or updated on December 1, 2011.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at
http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Global Business Services®	Redbooks®	Smarter Cities®
IBM®	Redguide™	Smarter Public Safety®
Information Agenda®	Redbooks (logo) ®	

The following terms are trademarks of other companies:

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.