


SAFETY THROUGH SYNERGY

WITH INTER-AGENCY
COLLABORATION

TABLE OF CONTENTS



01 Executive Summary

02 Introduction

04 The Promise
of Big Data

06 Making Sense
of Big Data

08 Helping Agencies Talk
to Each Other

10 The Gold Standard:
Situational Awareness

12 NEC Public Safety

EXECUTIVE SUMMARY

With increasing urbanization, our cities are growing larger, more complex and less safe. Governments and city planners must be prepared for a wide variety of threats to public safety, ranging from terrorism to natural disasters. As cities become more densely populated, authorities must also look for solutions to improve the quality of city living.

The ability to collect data and extract information from it provides tremendous potential to make cities safer and more livable. We now have the technological capacity to collect enormous amounts of intelligence about our environment and to mine it for patterns and correlations that will guide emergency responses and improvements to key city services. A silo mentality and the lack of a dedicated system for data sharing, however, are major barriers to dynamic information flow between government agencies.

Technology can now play a crucial role in encouraging and enabling inter-agency collaboration. A state-of-the-art, end-to-end inter-agency collaboration framework bypasses bottlenecks of human response time and red tape between government agencies, allowing for swift action to be taken.

- a. **The framework will channel data from a city-wide network of smart sensors to the appropriate agencies for processing.** This data will come in wide variety of formats, ranging from surveillance images to newer, non-traditional data such as social media activity and citizen feedback.
- b. **The framework will incorporate big data analytics to extract useful, actionable information from the sea of available data.** A major advantage to the analysis of big data is the power to extract hidden patterns and unknown correlations. But big data platforms should also have mechanisms in place to protect the privacy of the individual.
- c. **Based on the results of the analytics tools, the framework will then recommend a course of action, and set it in motion using machine-to-machine communication capabilities.** For a fully automated response, components of the framework should communicate with each other.
- d. **Ultimately, the goal of the inter-agency collaboration framework is to achieve situational awareness.** This involves a multifaceted understanding of how the situation is developing in both space and time, allowing the framework to play a critical decision making role in coordinating emergency responses.

INTRODUCTION

Safeguarding our growing cities

Cities are the heartbeat of a country. For the first time in human history, the majority of the world's population lives in these centers of economic, political and cultural activity. Urbanization will continue to be a trend for the foreseeable future, and cities will grow in population, geographical size and interconnectedness. By the middle of the 21st century, the world's urban population will have almost doubled in size, expanding from approximately 3.4 billion in 2009 to 6.4 billion in 2050, when seven out of every ten people will live in a city.¹ Almost all of this growth will occur in cities of the developing world.

With urban complexity and dense populations comes an increased level of threats to public safety. These threats may arise from a wide variety of sources, including violent crime, terrorism, cyber-attacks and natural disasters, and have the potential to endanger both human lives and key city installations. Governments, city planners, private companies and individuals alike will thus need to be well equipped to prepare for, respond to, and recover from these diverse security challenges.

Besides dealing with emergency situations, governments also face the challenge of making our increasingly dense cities more livable. Seemingly mundane problems such as traffic congestion, inefficient public transport, and air and noise pollution not only make daily life unpleasant, but in the long run may also adversely affect the ability of a city to compete globally. In addition, citizens also increasingly demand swifter and more effective resolutions to emerging problems. These expectations may be heightened by the widespread use of social media to document the situation on the ground as it unfolds.

The need for inter-agency collaboration

Technology will be an essential driver of solutions aimed at making our cities safe and more livable. Sprawling, city-wide sensor and communication networks already have the capacity to collect multiple types of data for public safety agencies to act upon. In the wake of September 11 and other terrorist attacks, New York City and London have deployed vast networks of surveillance cameras to detect suspicious activity. Government agencies must now find ways to interpret this exponentially growing volume of intelligence and use it to mount effective responses in a timely and effective manner. Achieving such a response typically requires a coordinated, interdisciplinary effort involving multiple agencies.

Inter-agency collaboration is particularly crucial during an emergency situation. In response to a fire in a densely populated area, for example, city authorities may need to activate the fire service, police, emergency medical services and transport, utilities and telecommunications companies. This coordination becomes even more complicated during larger-scale situations such as terrorist attacks. Apprehending a terror suspect who has entered the country, for example, requires agencies such as law enforcement and emergency services to obtain and analyze information in the shortest time possible in order to maintain control over a rapidly shifting situation.



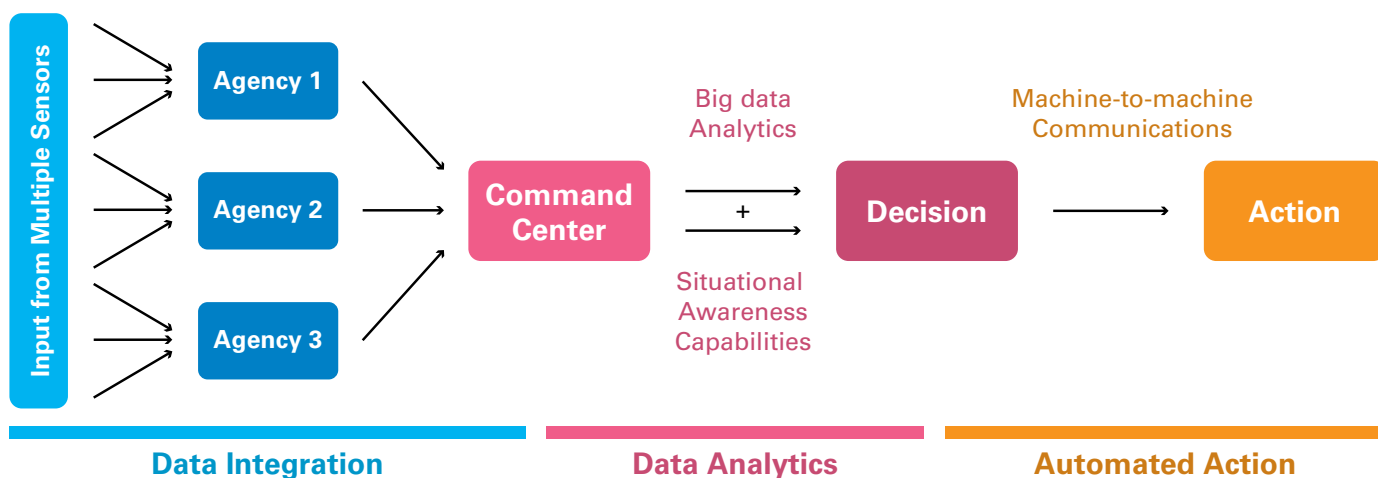
In practice, however, agencies are more likely to perform their respective functions in silos. For example, each may separately acquire technology or infrastructure to carry out its own monitoring and control activities, ignoring potential overlaps and opportunities for collaboration. Without a dedicated system for data sharing, duplication of effort and resources typically results. In addition, data collected from one agency provides an incomplete picture of the situation, and must be combined with other data types from different sources before meaningful conclusions can be drawn.

Better data analytics capabilities are also required – the sheer volume of data available far exceeds what human operators can process within a short response window, resulting in bottlenecks in the flow of information between agencies and hence delays in response times.

In contrast to government agencies addressing issues individually, a framework for inter-agency collaboration would consider the city as a whole, treating it as a single platform for service delivery (Figure 1). A command center incorporating state-of-the-art technologies would be able to seamlessly filter and channel data from a large number of sensors for processing. To allow this data to be analyzed and acted on, the framework would also incorporate sophisticated analytics capabilities, machine-to-machine communication and networking tools, all within a single interface. Ideally, the data collection, integration, analysis and subsequent decision on a course of action should be a fully automated, seamless process.

For example, the command center of an early warning system for a city prone to flooding would gather data from various sensors such as surveillance cameras, water level gauges, rain gauges and seismometers. It would then integrate and analyze the data to determine the likelihood of a flood. If the data suggests imminent flooding, the command center would then be able to issue an evacuation order for the affected population.

Figure 1: Inter-agency Collaboration Framework



THE PROMISE OF BIG DATA

Sophisticated sensors

While information used to be a scarce commodity, this is no longer the case. We are now well equipped not only to gather and store vast amounts of data about our surroundings, but also to analyze and glean meaningful insights from it.

To guard against terrorist attacks and criminal violence, governments have blanketed cities with thousands of security cameras capturing video footage of roads, street corners, transportation networks and other public spaces. London's "Ring of Steel" surveillance system employs almost half a million cameras, roadblocks and licence plate readers to monitor anyone entering or leaving the city center. After September 11, New York City implemented an initiative modeled on the "Ring of Steel" to survey lower Manhattan with thousands of private and public security cameras, which are monitored by authorities around the clock.²

But data collection is not just limited to images from surveillance cameras. Sensors that gather data of all sorts are ubiquitous in our society today. A smartphone, for example, is loaded with sensors that can detect the touch of a user's fingers, his geographical location, the direction in which he moves, and whether he is holding the phone horizontally or vertically. Ideally, sensors should be "intelligent" enough to relay that information, in real time, to a command center for analysis. Newer generations of sensors may go one step further and integrate processing power, in effect making them miniature computers.

Data gathered by sensors can be used to direct emergency responses from a city's emergency response command center. The sensor network of an early warning system for dangerous weather conditions, for example, can monitor environmental parameters as diverse as temperature, precipitation levels, air and water quality, wind speed and seismic vibrations, and issue an evacuation order if the situation calls for one. Sensors are also critical in industrial environments such as chemical factories, where a gas or chemical leakage must be detected early to avoid disaster.

Sensors can also equip citizens with useful, time-saving information, especially in densely populated cities where traffic congestion is a major problem. To help drivers and pedestrians plan their routes in advance, traffic conditions can be monitored in real time through a variety of methods, including GPS-based tracking and motion and road-embedded sensors. Commuters can also decide whether or not to drive based on the availability of parking spaces in the city. Seoul's real time traffic monitoring system, for example, gathers location data from 25,000 GPS-enabled taxis to calculate vehicular traffic speeds on the city's roads.³

To help cities stay sustainable, sensors can also be deployed throughout a city to reduce a city's energy consumption and improve the efficiency of its essential services. For example, street lighting can be controlled and weather-adapted based on data from sensors that detect ambient light conditions, and trash collection services can be optimized using sensors that monitor rubbish levels in bins.



Social media filtering and citizen feedback

In addition to images from surveillance cameras and physical data, 21st century society is also awash with cyber-information – social media updates, email messages, internet search history and websites visited, for example. These newer forms of data are no less valuable for authorities seeking to improve public safety, and can provide important insights into public opinion and sentiments on the ground in real time.

During major public events such as protests, parades or sporting events, for example, filtering publicly available social media feeds on Facebook and Twitter would provide a clearer picture of events unfolding on the ground and allow law enforcement agencies to deploy crowd control personnel in a swift and effective manner should the need arise.

Analyzing social media activity of criminal gang members and their associates can also provide law enforcement agencies with intelligence about current or potential hotspots of criminal activity, or tip them off about the whereabouts of a suspect. As part of its anti-terror efforts, the British government recently proposed legislation that would allow it to store and filter information about the public's email and social media communications. It is expected that security agencies will be privy to information such as who is talking to whom and when the conversations are occurring, but not to the actual content of the communications.⁴

On a more mundane level, keeping track of citizen feedback and complaints on social media can also help government agencies to improve the quality of important services such as public transport, healthcare and education.

Traditionally, data collection and filtering has been carried out by government agencies or their contracted companies. This top-down approach is an essential step towards building a smart city, but in the long run may not be sufficient, given the growing size and complexity of our cities. An important future trend is thus for governments to engage citizens in the data gathering process, a concept which is starting to be implemented in some parts of the world.

The Open311 interface⁵ used by some cities in the United States and Europe, for example, builds on the concept of the 311 telephone numbers used to access non-emergency municipal services in the United States. Open311 allows citizens to report a huge range of non-emergency issues – potholes, broken traffic lights and graffiti, for example. It also has a smartphone application that people can use to send in photographs of the situation as it unfolds. Because it is an open platform, third party developers can write their own apps to address specific issues in the community. This example illustrates how a combination of centralized technology and social engagement can be used to improve city services.



MAKING SENSE OF BIG DATA

Integrating and analyzing the information

The thousands of sensors making up the city-wide network will most likely be under the purview of different government agencies or private companies. Data from one or a few agencies, however, does not provide a complete picture of the situation, and a major challenge for inter-agency collaboration is to seamlessly integrate large volumes of data from multiple sources.

Big data integration typically involves establishing a command center to which all sensors will relay their data. Such a strategy should be amenable to being rolled out on a large scale: in a major metropolitan area, for example, the framework could be hierarchical, with several smaller command centers aggregating data from their respective districts, and then reporting this to a central command center for further analysis.

When integrating information from thousands of sources, data quality is a key consideration. Sensors can become compromised for a variety of reasons, for example in the event of a hacking attack. Making decisions based on data from these sensors leads to errors, and is a waste of time and resources to boot. Thus, while scalability is important, the ability of the command center to maintain granularity of control over individual sensors is also critical, and a command center should be able to detect compromised sensors and reach out to shut them down.

To extract meaningful information from a sea of data, the command center should also incorporate big data analytics capabilities. A major advantage to the analysis of tera- or petabytes of data is the power to extract hidden patterns and unknown correlations, a feat that would not be possible with smaller datasets.

Big data analytics is becoming increasingly sophisticated. Video analytics tools that perform facial and behavioral pattern recognition, for example, far outperform human ability to sift through thousands of images. These analytics tools have been instrumental in efforts to apprehend suspects, for example during the aftermath of the Boston Marathon bombing in 2013.⁶ Law enforcement agencies in many cities have also adopted predictive analytics combined with traditional police work to target crime.



Case study: NEC's Bring Your Own Engine smart pooling solutions

City planners today face the twin problems of heightened security requirements and limited resources. These limitations have prompted NEC to develop a smart pooling platform, based on the "bring your own engine" concept. Authorities can plug in their own specific analytic engines, analyze relevant raw data and turn it into actionable information.

In 2013, NEC and Tigre City in Argentina signed a memorandum of understanding to test NEC's smart pooling platform. Located 32 km from the Argentinean capital Buenos Aires, one of Tigre's challenges was the high volume of traffic throughout the city.

As part of the collaboration, NEC helped the city develop a 22-seat command and control center that linked up various components such as street surveillance, vehicle tracking and force coordination. From the purpose-built Tigre City Operations Center, officers could view incoming information from NEC's advanced CCTV cameras, intelligent video analysis systems and data center.

An interesting aspect about the Tigre City project is the way it was rolled out. Rather than invest heavily on one technology, the project was deployed as part of a 36-month service contract. Hence, the city can plug in new innovations as they become available over time.

Addressing privacy concerns

Although most citizens recognize the tremendous potential of big data to improve public safety and the quality of city living, the collection of data on an unprecedentedly large scale will inevitably result in concerns about privacy, and about how the use of this data may negatively affect the individual.

A balance must be struck between providing government agencies with access to the data needed for public safety responses, and protecting the privacy of the individual. One way that this can be achieved is through the use of encrypted data and algorithms. These would allow authorities to match faces in a surveillance video with a database of suspects, without actually identifying other people in the video.

Data can also be "sanitized" or anonymized, meaning that it is purged of details that could potentially identify the individual. Such detail is often superfluous to the analysis – for example, the use of payment touch cards and surveillance video to track peak hour activity of a subway system only requires information about commuter volume, and not about the locations of individual persons. Data sanitization should be done at the earliest possible stage of data analysis to minimize the risk of a security breach.

Governments should also ensure that the information technology infrastructure supporting the big data initiative is equipped with adequate security and privacy controls. Checks or audits can be carried out on a regular basis to ensure that the system remains robust against threats such as cyber-attacks.

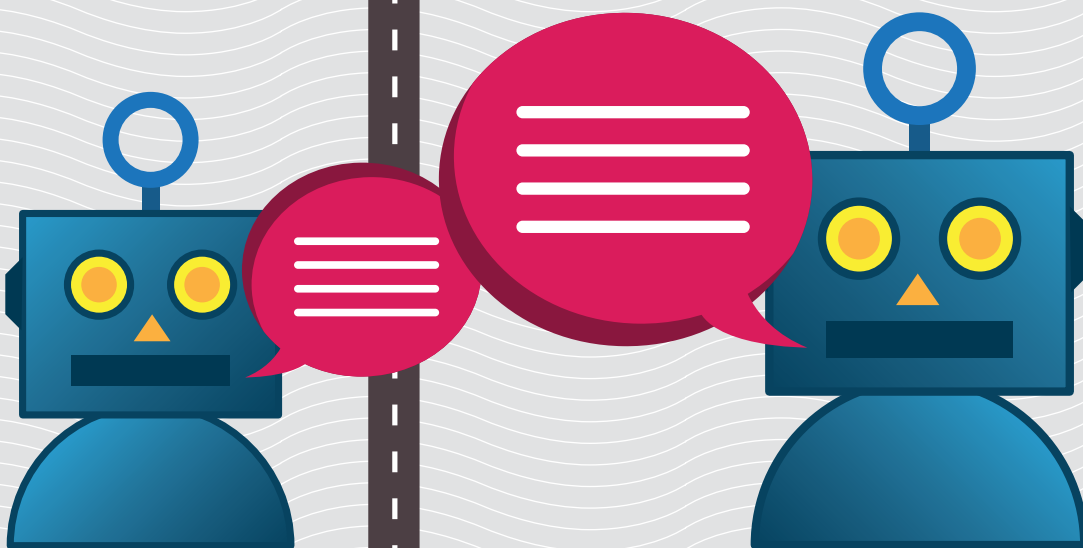
It is critical that privacy protection and good data governance practices be built into the system from the start. This is particularly relevant for social media analytics, and will go a long way towards building trust and convincing citizens that big data does not equate to "Big Brother."

HELPING AGENCIES TALK TO EACH OTHER

A key enabling technology that links up multiple government agencies is machine-to-machine communication. To build a seamless, fully automated emergency response framework, various components of the framework must contain embedded technology that enables them to talk to one another and to the command center, without human intervention.

The network of these communications between billions of physical objects – sensors and actuators, for example – has been termed the Internet of Things, and is expected to grow from 0.9 billion units in 2009 to 26 billion units in 2020, according to technology research firm Gartner. This growth will far outstrip that of other connected devices; for comparison, the number of PCs and mobile devices such as smartphones and tablets in use in 2020 is estimated at 7.3 billion units.⁷

Although the Internet of Things has not yet been widely adopted, it has enormous potential to transform the way in which cities function. When physical objects can both sense the environment and communicate with each other, they become valuable tools for coming to grips with complex, data-intensive problems. Since the information being exchanged can be limited to simple data points – a numerical value representing water level or wind speed, for example – the Internet of Things need not require as much bandwidth as current 3G or 4G networks. It would, however, have to be sufficiently robust to handle millions of interactions between network components, with minimal lag.



Case study: NEC to develop Safe City Test Bed in Singapore

The Safe City Test Bed project, spearheaded by Singapore's Ministry of Home Affairs and Economic Development Board, aims to develop state-of-the-art technology for use in improving public safety. In 2013, a consortium led by NEC Asia Pacific was one of four selected to develop Safe City Test Beds in Singapore.⁸

NEC's proposition is to build a complete, end-to-end inter-agency collaboration framework that uses technologies such as advanced data analytics, risk analysis and relationship modeling to allow agencies to integrate disparate information from various sources.

Participating government agencies include those in charge of emergency services (the Singapore Police Force and Civil Defence Force), environment and utilities (the National Environment Agency and Public Utilities Board) and transport (the Land Transport Authority).

NEC's solutions are expected to help these agencies to overcome infrastructural and technical barriers to inter-agency collaboration, optimize the use of manpower and improve situational awareness and anticipation of security threats.

In situations where time is of the essence, communication between machines avoids the bottlenecks of human response time and red tape between government agencies. For example, if a threat is detected in the central business district and the information relayed to the command center, the command center can in turn swiftly take control of electronic billboards in the area and use them to display evacuation instructions, even if they are under the jurisdiction of different public or private agencies. Perimeter access control is another application, where detection of non-authorized personnel in sensitive areas can automatically trigger a security response.

Harnessing machine-to-machine communication can also revolutionize how municipal facilities are used and managed. The ubiquitous components of key city infrastructure, such as lamp posts, water pipes and power cables, can become part of a data-generating sensor network that monitors numerous environmental parameters in real time. In San Francisco, street lighting is being transformed into an expandable, wireless communication network. Previously humble lamp posts will contain sensors that can monitor not only themselves, but also a wide range of other municipal facilities such as electricity meters, traffic lights, electric vehicle charging stations and parking spaces.

Before they can be adopted on any scale, the main challenge for Internet of Things applications is cybersecurity. Machine-to-machine networks and their components must be free of security loopholes that hackers or malicious software could exploit to gain access to data or to take control of the system. Governments and city planners should be aware of these potential risks, and ensure that their contracted service providers are able to implement robust safeguards against them.

THE GOLD STANDARD: SITUATIONAL AWARENESS

Ideally, the inter-agency collaboration framework should not merely be a command center that integrates and analyzes data from many different sources. Instead, it should provide authorities with a detailed and multi-faceted perspective of the situation on the ground, with respect to both space and time. It should also have reasoning capabilities, allowing it to play a critical decision making role in coordinating emergency responses.

This level of perception has been termed situational awareness, and is critical for understanding how events, information and one's course of action will impact goals and objectives, both at that point in time and in the near future. Situational awareness is particularly important in complex and changeable emergency situations, where poor decisions can result in serious consequences. Indeed, poor situational awareness is thought to be a major factor in accidents attributed to human error.

A key aspect of situational awareness is geospatial analysis, which adds timing and location to traditional data to create maps that show changes over space and time. In the past, workers responding to an emergency call to the fire department, for example, would only be told the bare minimum: the type of situation to which they were responding, and its location. An inter-agency collaboration framework capable of situational awareness, however, would also take the location's surroundings into account. For example, if the fire were next door to a chemical factory, boarding school or home for the elderly, it would alert and activate the relevant agencies should a special response be required. The system would also be able to keep track of environmental factors affecting the fire, such as wind speed and wind direction, and provide up-to-date reports to first responders using a map-based interface.



Response times could also be cut significantly by a situationally aware dispatch system. When an emergency call is received, the system would locate it on a map in the context of all open calls and available emergency response units in the area. It would then be able to recommend not only the closest unit, but also the one with the most relevant emergency response capabilities. While that unit is on its way to the location, the system would also be able to use real-time traffic information to direct it there via the fastest possible route.

Situational awareness can also be extremely useful in cases where the threat is not readily apparent. The accidental release of an odorless, colourless toxic gas, for example, could cause unexplained human casualties in the vicinity, prompting calls to the emergency hotline. An inter-agency collaboration framework would be able to call up information such as the names of businesses in the area, whether any of them have special permits for the use of chemicals, and building and fire safety inspections records that would detail the presence of chemical containers on the premises. These pieces of information, normally under the jurisdiction of disparate government agencies, would be invaluable for first responders to pinpoint the root of the problem and take the necessary course of action.

In addition to guiding immediate emergency responses, the integrated, context-aware analysis performed by an inter-agency collaboration framework would also allow authorities to make predictions of how the current situation would impact events in the near future. For example, if it is predicted that traffic congestion caused by flooding will result in a massive tailback affecting outlying areas several hours later, action could be taken to pre-empt the situation by diverting traffic away from the affected areas even before the congestion becomes apparent. Predicting these secondary “knock-on” or “domino” effects in advance enables the authorities to take advance action, and hence prevent the accumulation of negative consequences.

Case study: Situational awareness app aids firefighters in California

Wildfires are a major threat to lives and property in the Western United States, and have increased in number and severity over the last few decades. Firefighters in California are increasingly adopting a free web-based situational awareness app in their response to wildfires.⁹

The open standards-based app, Next-Generation Incident Command System (NICS),¹⁰ was developed by the Massachusetts Institute of Technology Lincoln Laboratory and the California Department of Forestry and Fire Protection.

During an emergency situation, NICS manages and disseminates data, including real-time vehicle locations, weather and terrain information.

Firefighters use the app to map out wildfires in real time and plan their responses accordingly, marking out features such as an incident perimeter, staging areas, evacuation zones, road blocks and division breaks. To facilitate inter-agency collaboration, these maps are immediately made available over the Internet to all levels of emergency responders and can be used on computers and mobile devices.

Although the app has mainly been adopted by firefighters, it can also be used by other public safety agencies such as law enforcement, emergency medical services and public utilities. Future improvements include the integration of plug-and-play apps from third party developers in the emergency response community.



NEC PUBLIC SAFETY

As cities grow and flourish, they also face increasingly complex challenges. City planners and governments need to find ways to respond to the immediate needs of their citizens, while also sustaining the effect for the long run.

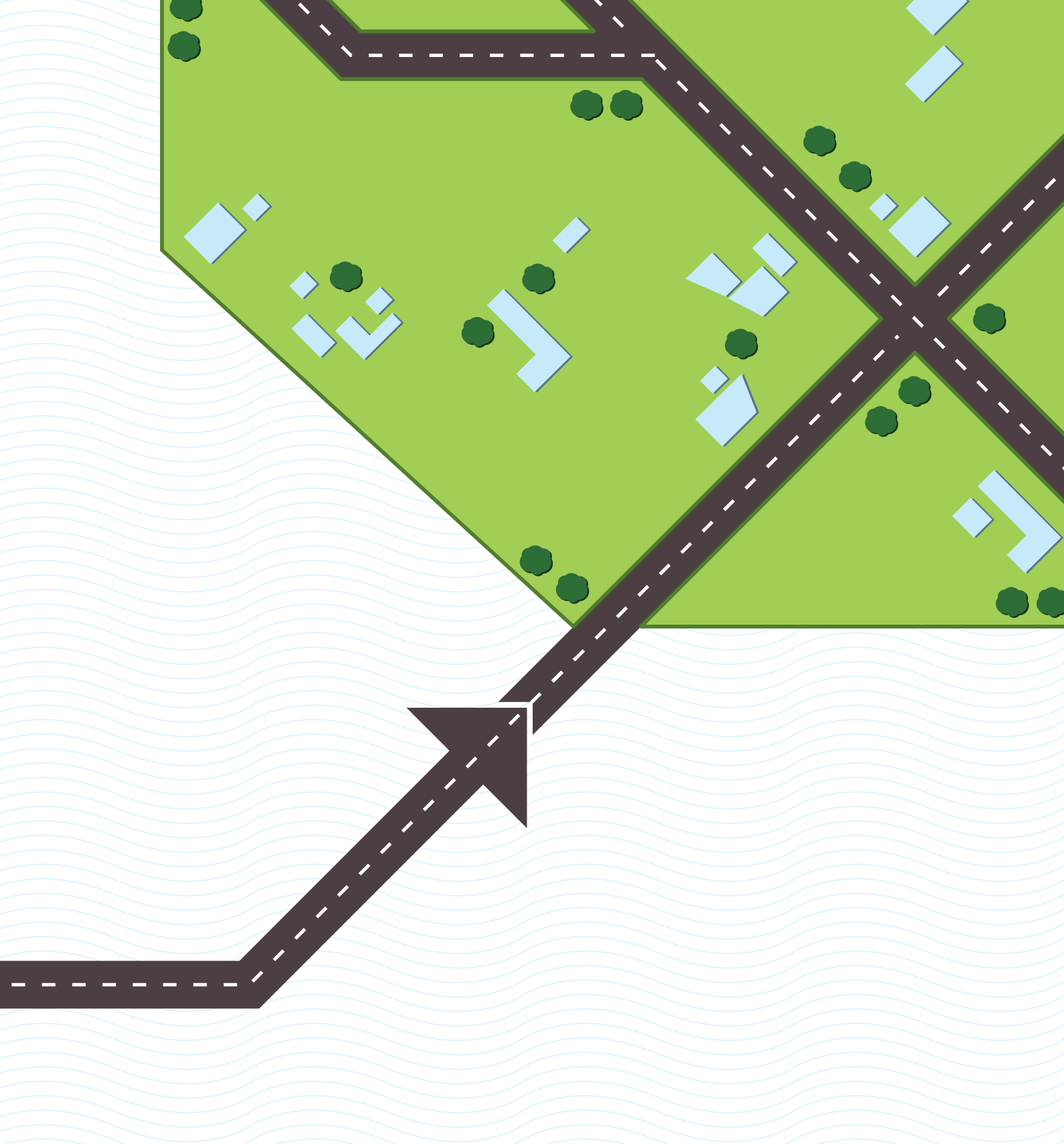
NEC has dedicated its resources to helping cities stay safe and sustainable. In situations of national importance, technology can play a crucial role, allowing city authorities to quickly take stock of a complex situation, and respond in an agile and timely fashion.

To keep cities safe, NEC has developed a comprehensive suite of public safety solutions in the areas of national identification, law enforcement, immigration, emergency and disaster response, and protection of key physical and cyber infrastructure. NEC's biometric identification systems, for example, are used by more than 480 customers in over 30 countries to protect border checkpoints such as airports and seaports.

With the rise of big data, along comes the challenge of interpreting the information collected. NEC is at the forefront of big data technology, with solutions for data collection, platforms for data exchange between agencies, operations center infrastructure, and powerful data analytics capabilities.

To help government agencies work more effectively as a team, our state-of-the-art machine-to-machine communication systems provide a seamless and scalable solution to integrate information from multiple sources, as well as decide upon a course of action.

So whether a city is looking to find ways to improve its emergency response capabilities, defend against physical or virtual threats, or use its energy resources more wisely, NEC can help. Our technologies maximize the potential of big data to create more livable cities of the future.



¹ Urban population growth fact sheet, World Health Organization Global Health Observatory.

² New York Plans Surveillance Veil for Downtown, New York Times, 2007.

³ The new smart city – from hi-tech sensors to social innovation, The Guardian, 2013.

⁴ Government plans increased email and social network surveillance, The Guardian, 2012.

⁵ Open311, <http://open311.org/>

⁶ After Boston: The pros and cons of surveillance cameras, CNN, 2013.

⁷ Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020, Gartner Inc, 2013.

⁸ Singapore to Develop and Test New Solutions for Safety and Security, Singapore Ministry of Home Affairs, 2013.

⁹ Free situational awareness app gaining traction among California firefighters, GCN, 2014.

¹⁰ Next Generation Incident Command System, <https://public.nics.ll.mit.edu/nicshelp/articles/about.php>

Contributors:

- Paul Wang (PhD), Chief Technology Officer, Global Safety Division, NEC Corporation.
- Woo Kang Wei (PhD), Technical Director of Inter-Agency Collaboration, Global Safety Division, NEC Corporation.
- Koh See Kiat, Business Development Director of Inter-Agency Collaboration, Global Safety Division, NEC Corporation.

About NEC Global Safety Division

NEC Global Safety Division, a business division within NEC Corporation, spearheads the company's public safety business globally. The Division is headquartered in Singapore and offers solutions in the following domains: Citizen Services & Immigration Control, Law Enforcement, Critical Infrastructure Management, Public Administration Services, Information Management, Emergency & Disaster Management and Inter-Agency Collaboration. Leveraging on its innovative solutions, the Division aims to help government and business make cities safer.

NEC Global Safety Division

Global Headquarters: 2 Fusionpolis Way, #07-01/02/03 Innovis, Singapore, 138634
For enquiries, please contact safety@gsd.jp.nec.com

nec.com/safety



Citizen Services & Immigration Control



Law Enforcement



Critical Infrastructure Management



Public Administration Services



Information Management



Emergency & Disaster Management



Inter-Agency Collaboration

Orchestrating a brighter world

NEC brings together and integrates technology and expertise to create the ICT-enabled society of tomorrow.

We collaborate closely with partners and customers around the world, orchestrating each project to ensure all its parts are fine-tuned to local needs.

Every day, our innovative solutions for society contribute to greater safety, security, efficiency and equality, and enable people to live brighter lives.

The information contained in this white paper is the proprietary and exclusive asset of NEC unless otherwise indicated. No part of this white paper, in whole or in part, may be reproduced, stored or transmitted without the prior written permission of NEC. Unauthorised use or disclosure may be considered unlawful. It is intended for information purposes only, and may not be incorporated into any binding contract. This white paper is current at the date of writing only and NEC will not be responsible for updating the reader of any future changes in in circumstance which may affect the accuracy of the information contained in this white paper. Some of the ideas in the paper are aspirational, and NEC is working towards realizing these ideas in our vision of making cities safer.