ACHIEVING INTEROPERABILITY IN PUBLIC SAFETY AND EMERGENCY RESPONSE IT/COMMUNICATION SYSTEMS

Robert I. Desourdis, Jr.
Science Applications International Corporation
United States of America

ABSTRACT

Interoperability is a measure of shared, trusted understanding that drives predictable collaborative action to achieve a common goal. Failed technological interoperability (e.g., radio interoperability) is not the root cause for failed interoperability as a whole – it is a symptom of the disease and not the disease itself. The nature of deficiencies in public safety and emergency response IT/communication systems today are identical to those documented in the congressional report investigating the successful Japanese surprise attack on the U.S. Pacific Fleet at Pearl Harbor in December 1941. This paper identifies the fundamental information-sharing deficiencies resulting in failed interoperability. It then presents a dual top-down/bottom-up approach for mitigating and eliminating these deficiencies, creating – for the first time – a documented best-practices information-sharing architecture across all public safety and emergency response organizations.

KEYWORDS: interoperability, public safety, emergency response, Pearl Harbor, best practices, organizational development, organizational effectiveness, business case analysis, cost-benefit analysis, enterprise architecture, operational view, system view, systems engineering and integration, training and exercises.

DISCLAIMER: The opinions expressed in this paper are only those of the author and do not necessarily represent those of Science Applications International Corporation or any other individual or organization.

1. DEFINITION OF INTEROPERABILITY

1.1 NEED FOR INTEROPERABILITY

The need for true civilian public safety and emergency response interoperability, which, throughout this paper, does not mean just radio interoperability, can be deduced from the same reasoning that has driven major national resources into military capabilities to support the warfighter. Many countries have faced ignominious military disasters, and insist on not being surprised again. “No more Pearl Harbors” is one expression that not only states this resolve, but largely reflects the investment in all aspects of military capability and sustainment worldwide. However, with the advent of chemical, biological, radiological, nuclear, explosive (CBRNE) weapons of mass destruction (WMD) and well-armed kamikazes aimed at the civilian populations, it is incumbent on the world’s
governments to focus even more energy, resources, and best-practices for the optimization of public safety and emergency response IT/communication systems.

Several categories of communications interoperability for public safety and emergency response responders-receivers\(^2\) have been defined as follows:

- **Modes of routine intra-agency operability:**
  - Normal operations within a discipline.
  - Communications that are rehearsed and practiced every day.
  - Day-to-day patrols/duties and responses to dispatches from emergency call centers.
  - Task force operations within a discipline/agency for a specific mission.

- **Modes of interagency interoperability:**
  - Day-to-Day:
    - Communications that are rehearsed and practiced every day.
    - Routine operations with neighboring agencies to provide support or backup. It is estimated that this form of interoperability makes up 90 percent of an individual first responder's multi-agency activities.
  - Task Force:
    - Cooperative effort among mixed yet specific agencies/disciplines.
    - Extensive preopening with practice.
    - Operations that are planned/scheduled and proactive.
    - Operations that have a common goal, common leader, and common communications.
  - Mutual Aid:
    - Major event that causes a large number of agencies to respond and requires considerable coordination.
    - Major event that requires response from multiple jurisdictions from the local level to the state and national level.
    - Communications that operate under a state or regional mutual aid pact.
    - Operations that are usually not planned or rehearsed but are reactive to the situation.\(^3\)

In recent years, the developed countries have been investing significantly in improving public safety and emergency response interoperability, with the primary focus on radio communications. One pervasive definition defines interoperability as:

... the ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice and/or data with one another on demand, in real time, when needed.\(^4\)

Limiting the interoperability definition represents efforts to address inadequate communications coordination between the mobile operations of public safety and emergency response personnel, but it narrows the scope of the problem to “radio” and “exchanging voice and/or data.” More importantly, it mistakenly focuses attention on curing the apparent lack of radio interoperability – which is only a *symptom* of the real problem – rather than concentrating on the need to identify and fix the underlying root *cause* that is failed information sharing. Radio interoperability would not have become an issue in public safety or emergency response had this fundamental cause not been a driving factor. In this paper, we will identify the cause as basic historic deficiencies in people and processes and describe techniques to mitigate and eliminate these
deficiencies. The goal of this paper and the associated work is to achieve true interoperability in public safety and emergency response IT/communication systems.

1.2 REAL INTEROPERABILITY

By broadening the definition from radio interoperability alone, we begin to move closer to the essential understanding of real interoperability that we will address in this paper. The Institute of Electrical and Electronic Engineers defines interoperability as:

The ability of two or more systems or components to exchange information and to use the information that has been exchanged.\(^5\)

This definition expands the scope beyond “radio” – implying all forms of “exchange” are included, and it includes reference to another important term, namely information, not just voice or data. Perhaps more importantly, it includes the phrase “to use the information that has been exchanged [Italics added].” To this end, the need and definition of “command and control” and the communications required to support it can be further refined as follows:

Public safety operations follow a command and control hierarchy that allows public safety personnel to work seamlessly on situations that may begin small, but can evolve into large incidents, requiring many resources and assistance from numerous jurisdictions. As an incident grows in magnitude, the incident commander has to know what resources and capabilities are becoming available for use. Each of the first responder disciplines may have their own branch commander at a large incident, and these branch commanders must be able to coordinate, communicate, and share information with the overall incident commander.

The communications systems that support these operations must also be capable of the same command and control features.

a. Incident command structure the communications systems must support the agency's incident command policies.
b. System administration of users
   the communications systems must allow authorized system administrators, as well as incident and branch commanders, to establish user profiles for network access and usage, depending upon the role that the public safety user is asked to satisfy during an incident.
c. User identification and location
   the communications systems must provide user identification to others during communications and, when required, must provide user geo-location information to incident commanders and other authorized resources.

Finally, the system must allow communications and information sharing between incident command and/or unified command operations with an Emergency Operations Center (EOC). In some instances, access on-demand is required by the EOC to Geographic Information System (GIS)-based displays, video, and communications as they are happening at the incident.\(^6\)

Note the key phrase “information sharing,” which is at the heart of true interoperability.

A recent and comprehensive review of interoperability definitions provides many variations of definition for the term interoperability.
For nearly thirty years, both government and industry have actively explored research on interoperability measurement with the goal of creating a straightforward way of measuring, reporting, then improving the interoperability of complex networks of people, equipment, processes and organizations. Researchers have created frameworks and models, proposed measures, described levels, and listed a variety of qualitative factors in support of an interoperability measure. Within extant interoperability research, the authors’ research has uncovered nearly three dozen definitions of interoperability, over five dozen distinct types of interoperability, numerous interoperability attributes, and fourteen foundational interoperability measurement models and methodologies. At least eleven research groups have been the centers-of-gravity for interoperability measurement research. …

After reviewing 34 definitions, these researchers pointed out that interoperability spans people, equipment, processes and organizations, and that it has been extensively studied. Several of these definitions include a key element of the aforementioned IEEE definition, that the exchanged information is used to achieve some common goal. This common public safety and emergency response goal is one or more of the following objectives:

- Prevent – Through intelligence, sensors, or other predictive means, be able to interdict manmade threats and reduce or eliminate the impact of natural events
- Detect – If prevention fails, determine the realization of a manmade threat or natural disaster – as well as its potential impacts – as soon as possible following its evolution or instantaneous occurrence
- Protect – Using in-place or executable resiliency measures, maximize defensive measures to minimize the initial impact of manmade incidents or natural events
- Alert – Provide instantaneous alerting with action-oriented situational awareness
- Respond – Take action to minimize scope, protect life and property, mitigate (manmade or natural) cause, and maintain situational awareness
- Recover – Restore/improve pre-event conditions and re-establish preparedness

The fact that the information is used – combined with the importance of people in the definition – emphasizes the importance of trust. In other words, interoperability requires that people will trust the use of the information exchanged according to established processes. This element of trust, though implied, does not occur explicitly in any of the 34 definitions identified in the interoperability study above. It is often assumed in the military domain, but it is a critical factor not always present in the civilian domains. Trust will nevertheless be prominent in our definition of interoperability used throughout this paper.

The IEEE definition is a major improvement to the radio-only version, but it is not yet an adequate definition for our purposes. Another broadening of our definition is to see interoperability as:

... a measure of the degree to which various organizations or individuals are able to operate together to achieve a common goal. From this top-level perspective, interoperability is a good thing, with overtones of standardization, integration, cooperation, and even synergy.
Interoperability specifics, however, are not well defined. They are often situation-dependent, come in various forms and degrees, and can occur at various levels—strategic, operational, and tactical as well as technological. They are also far more likely to be recognized when interoperability problems emerge and taken for granted when such problems do not.8

The key words here are *measure*, the focus on organizations or *individuals*, and their ability to *operate together* to achieve a *common goal*. In addition, this definition addresses strategic, operational, tactical, and technological elements—defining the scope of planned action and capabilities that the interoperability measure must consider. Also, the authors point out that interoperability is apparent in its absence, but otherwise overlooked. This statement shows the difficulty of establishing a quantitative measure other than the simple binary rating of interoperable or *not* interoperable.

**1.3 COMPLETING THE DEFINITION**

A valuable refinement of many specific underlying practical elements of interoperability has been developed that must be included in our understanding, that is:

Interoperability is a “cross-cutting concern” which must be implemented pervasively if it is to be effective. Yet because it is cross-cutting, it is typically considered out of scope by individual projects or programmes, since it involves interaction with other projects or programmes that are outside the boundary of the given effort. It must therefore be motivated and governed by mechanisms that transcend normal project and programme boundaries.9

A critically important term worth noting is *pervasive*, denoting that all organizations, entities, and individuals involved in achieving the common goal must be included. Here, the authors illuminated a key reason for failure of government and commercial programs and projects to address interoperability: it is often “out of scope” of individual projects. Often, various levels of government are not capable of establishing the necessary interoperability framework for these programs and projects, perhaps not aware that it is their responsibility to do so.

Several key practical elements needed to achieve interoperability have also been defined.

In order to interoperate meaningfully, organizations must have compatible data definitions and interpretations, terminology, business processes, organizational cultures, and policies concerning privacy, access, transparency, accountability, etc. Achieving true interoperability therefore requires the alignment of these semantics across all interacting organizations and their systems. Such alignment requires each organization, sector, and community of interest to define and codify its own semantics and to establish appropriate correspondences with the semantics of any other such entities with which it interacts. This in turn requires cross-organizational, cross-sector, and cross-community interaction and negotiation. Because this process is labour intensive and involves significant intellectual effort, it requires considerable lead time and so should be started as early as possible.10
The Rand Europe authors of these statements recognized that there must be shared understanding of exchanged information. Even this advanced characterization of interoperability falls (just) short of including trust, which is a fundamental element of holistic interoperability. The individuals and entities (via formal agreement) will trust the shared information to the point of acting on it in a coordinated way. In other words, the individuals and their entities must be willing to operate together, or collaborate, through the exchange of trusted information. This exchange could be on a

- Moment-to-moment basis during tactical operations, such as a law enforcement task force sweep, a multi-alarm fire or wildfire, or a mass-casualty incident, in which voice, data, and video are shared.
- Day-to-day basis, such as awareness of ongoing operations in the region, local minimal incidents and responding entities, recent incidents or events, upcoming weather, community events, etc.
- Continuum-of-time operations repeated at intervals from day-to-day through weekly, monthly, yearly, and beyond (e.g., 100-year storm).

Compiling the above-mentioned elements of our interoperability definition into one phrase suggests that interoperability measures the extent of trusted, shared understanding among public safety and emergency planners and responders collaborating (e.g., operating together) to achieve a common goal. To complete this definition, we must further expand each of the terms used in it.

By collaboration, we mean engaging in predictable coordinated actions to achieve a common goal. By predictable, we mean that given the exchange of trusted shared understanding, each entity can – based on training and standard operating procedures (SOPs) – predict the specific actions that will be performed by entities sharing that trusted understanding. These entities employ planners and responders/receivers that belong to organizational entities spanning many different

- Public safety and emergency response disciplines with the associated diverse goals, objectives, operating techniques, semantics, tools, training, etc.
- Levels of government, commercial, non-profit, and volunteer organizations.
- Diverse capabilities, responsibilities, operating procedures, semantics, priorities, policies, and resources.

Finally, we can make the following definition for the purposes of this paper:

**Interoperability is a measure of shared, trusted understanding that ensures predictable coordinated action among organizations collaborating to achieve a common public safety and emergency response goal.**

The critical success planning factors necessary to achieve interoperability have been shown to be\(^1\):
• **Governance** includes all aspects of the governance structure mandated by the leadership to empower stakeholders to use, improve, and implement their operational and system architecture.

• **Resources** – all aspects of resources and resource planning for interoperability Architecture, including funds for acquisition and sustainment (operation and maintenance), people, and infrastructure.

• **Approach** – all the best practices needed to design interoperable capability, such as organizational development/effectiveness, enterprise architecture practice, systems engineering and integration practice, program and project management, test and verification practice, etc.

• **Architecture** – this category includes the critically important integration between people and technology in the interoperability architecture, including:
  - All operational aspects, e.g., expertise, experience, SOPs/guidelines and timelines, integrated training and exercises, etc., and related operational standards, intended to prevent, detect, protect, alert, respond, and recover
  - All physical facilities, including structures and hardware/software systems, physical infrastructure (location, security, facilities, networks, etc.), and related technical standards, to provide trusted, shared understanding

• **Performance** – the detailed quantitative performance requirements for interoperability to be achieved: speed, accuracy, reliability, sustainability, and resiliency.

• **Acceptance** – all aspects of getting “buy in” from all levels of government leadership and the community as well as first responder leadership/organizations, responders/receivers, the media, and the public – all to establish shared trust.

Each of these planning elements is essential to achieving interoperability.

2. **WORLD INTEROPERABILITY MODEL**

2.1 **THE PEARL HARBOR DEFICIENCIES**

It is hard to imagine that despite the strategic warnings regarding an impending attack from multiple sources, including newspapers, diplomats, counterspies, Japanese diplomatic communications intercepts, consulate wire taps, radio signal intelligence, and accurate threat analysis and prediction, that the Washington, D.C., and Hawaiian military authorities were completely surprised on December 7, 1941. Several in-depth investigations of the Pearl Harbor attack followed. The congressional investigation and resulting report drafted by Assistant Counsel Edward P. Morgan present a detailed summary of the causes for failed American preparedness and alertness. Morgan’s
report identified the 25 deficiencies described in Table 1, which ultimately traced the disaster to failed leadership. As Prange et al states in “Primarily a Failure of Men,” Chapter 16:

One cannot understand the defeat which the United States suffered on December 7th, 1941, by attempting to analyze it in terms of economics, sociology, technology, or any other of history’s neat pigeonholes. It arose from the nature of the men involved. Ferguson [Senator Homer Ferguson] and his fellow Republican member of the congressional committee, Senator Owen Brewster of Maine, recognized this in their minority report: “In our opinion, the evidence before this committee indicates that the tragedy at Pearl harbor was primarily a failure of men and not of laws or powers to do the necessary things, and carry out the vested responsibilities.”

In presenting these failures, Prange et al characterized Morgan’s report:

The final report explained that the committee posed these points “not for their novelty or profundity but for the reason that, by their very self-evident simplicity, it is difficult to believe they were ignored.” Morgan confined himself strictly to factors illustrated by the attack, producing chapter and verse to back them up. The applicability of these points far transcends Pearl Harbor, so they deserve serious review...

<table>
<thead>
<tr>
<th>No.</th>
<th>Failure of …</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Organization</td>
<td>Multiple parallel organizations with ambiguous authority</td>
</tr>
<tr>
<td>2</td>
<td>Assumption</td>
<td>Information-sharing convention is not known or understood, but appropriate sharing to avoid disaster is assumed</td>
</tr>
<tr>
<td>3</td>
<td>Omission</td>
<td>Information-sharing distribution is incomplete, people and entities excluded</td>
</tr>
<tr>
<td>4</td>
<td>Verification</td>
<td>Commands/information sent, no follow-up to ensure understanding and action, capabilities or actions are assumed and not verified</td>
</tr>
<tr>
<td>5</td>
<td>Supervision</td>
<td>Provide close supervision to verify understanding and predictable action, often not performed – compliance assumed</td>
</tr>
<tr>
<td>6</td>
<td>Alertness</td>
<td>Heightened alert is undermined by repeated training and exercises</td>
</tr>
<tr>
<td>7</td>
<td>Complacency</td>
<td>Vigilance relaxes from the day-to-day lull of “business as usual,” a &quot;what-could-possibly-happen (?)&quot; or “things-are-good-enough” attitude</td>
</tr>
<tr>
<td>8</td>
<td>Intelligence</td>
<td>Centralize intelligence services with tailored dissemination of intelligence products, too many independent sources of collection and analysis</td>
</tr>
<tr>
<td>9</td>
<td>Attitude</td>
<td>Superiors do not engage in open dialogue with peers and subordinates, the superiors act superior to their subordinates (arrogance)</td>
</tr>
<tr>
<td>10</td>
<td>Imagination</td>
<td>“Worst-case” scenarios not included in preparedness and response planning</td>
</tr>
<tr>
<td>11</td>
<td>Communications</td>
<td>Information exchanged is ambiguous, convoluted, or</td>
</tr>
</tbody>
</table>
### TABLE 1  THE PEARL HARBOR DEFICIENCIES

<table>
<thead>
<tr>
<th>No.</th>
<th>Failure of …</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Paraphrase</td>
<td>Messages altered according to assumption with no verification</td>
</tr>
<tr>
<td>13</td>
<td>Adaptability</td>
<td>Alert and response thresholds are not matched to the known threat environment</td>
</tr>
<tr>
<td>14</td>
<td>Disclosure</td>
<td>Intelligence so protected that it is inaccessible to those who urgently need it, rather than converting products to actionable information while protecting “sources and methods”</td>
</tr>
<tr>
<td>15</td>
<td>Insight</td>
<td>Inadequate understanding of the threat and capabilities to address this threat lead to underestimated risk</td>
</tr>
<tr>
<td>16</td>
<td>Dissemination</td>
<td>Information is not provided to subordinates who need to know</td>
</tr>
<tr>
<td>17</td>
<td>Inspection</td>
<td>Leaders do not know or understand their personnel and critical systems</td>
</tr>
<tr>
<td>18</td>
<td>Preparedness</td>
<td>Prepare for consequences of what a threat might do, instead of what it could do</td>
</tr>
<tr>
<td>19</td>
<td>Consistency</td>
<td>Official direction is contradicted by unofficial speculation from authorities</td>
</tr>
<tr>
<td>20</td>
<td>Protectiveness</td>
<td>Individual or organizational one-upmanship for real or perceived self-benefit, a “me-first-me-only” behavior</td>
</tr>
<tr>
<td>21</td>
<td>Relationships</td>
<td>Personal friendships inhibit identification and resolution of deficiencies or gaps and are falsely interpreted by onlookers as interoperability</td>
</tr>
<tr>
<td>22</td>
<td>Priority</td>
<td>Failure to prioritize critical needs over day-to-day activities</td>
</tr>
<tr>
<td>23</td>
<td>Reporting</td>
<td>Subordinates fail to report information up the command chain</td>
</tr>
<tr>
<td>24</td>
<td>Improvement</td>
<td>Failure to identify gaps, particularly in worst-case scenarios, and correct them</td>
</tr>
<tr>
<td>25</td>
<td>Delegation</td>
<td>Responsibility is delegated with inadequate authority to act, and those who act from initiative are chastised – reducing subordinate’s will to do so when needed</td>
</tr>
</tbody>
</table>

The Pearl Harbor deficiencies minimized the level of *shared, trusted understanding* among the commanders in Washington and Hawaii on December 7, which meant there would be inadequate *predicable collaborative action* from the moment Fuchida’s first wave approached Oahu.

Leaders and planners in all public safety and emergency response organizations and layers of government should review these deficiencies and design operating procedures and IT/communication system architecture to mitigate or eliminate them from their own organizations. More than any other time in history, public safety and emergency response architecture should explicitly account for these natural human failures in their

- Detailed operational and IT/communication system architecture requirements, including the necessary activities and necessary information flows.
- Development, procurement, implementation, verification, quality, sustainment, and continuous improvement processes.

This capability and the willingness to ensure steps to mitigate and eliminate the Pearl Harbor deficiencies must become a critical part of their job description – rather than being further ignored over 60 years after the events at Pearl Harbor.

Each deficiency signifies potential gaps between best-practice interoperability and business as usual. Unfortunately, failure to identify and correct (see Deficiency #24) any one gap – even a minor gap – in governance, resources, approach, architecture, performance, or acceptance, could lead to future catastrophes in a CBRNE WMD world. Governments must empower leaders who will seek out and fill these gaps regardless of political sensitivity, ensuring that future public safety and emergency response architecture. In summary, Prange et al state that:

Careful consideration of Morgan’s points reveals that many of them are separate facets of a single problem – the failure to communicate. The aspect of the matter may well stand as one of the basic causes of the Pearl Harbor tragedy, second only to the failure to believe in its possibility. One by one these failures pass in sorry review: failure to ensure understanding, failure of seniors to supply all available relevant information to juniors; failure to supervise and follow through; failure of juniors to be sure they understand their seniors; lack of clarity of expression.

The failure of 1941 to apply such principles as Morgan’s cost the United States dearly at Pearl Harbor; hence they must be considered as lessons to be learned from the debacle. Any country, any organization, indeed any individual, can profit by pondering these points. ¹⁶

If Morgan had performed an in-depth analysis of Titanic (1912), Lusitania (1915), Poland (1939), Coventry (1940), Russia (1941), Bastogne (1944), Hiroshima (1945), Beirut (1983), 9-11 (2001), Madrid (2004), Tsunami (2004), Katrina (2005), or Mumbai (2008), and countless other even references, he would have doubtless found the same deficiencies. He would have concluded that leaders were destined for failed interoperability, and that the many deficiencies evident from his Pearl Harbor investigation were simply defining natural characteristics of all human organizations.

As a consequence of Prange and his co-author’s defining work, no better example of failed interoperability has been so painstakingly documented. As stated previously, anyone who leads or plans anything involving human interaction ought to ensure they read these texts, improve their people, processes, and tools from these lessons not yet learned. Recalling our definition of interoperability, a measure of shared, trusted understanding that ensures predictable coordinated action among organizations collaborating to achieve a common public safety and emergency response goal, there is no doubt that it was lacking in Washington and Hawaiian preparedness at 0749 December 7, 1941, Hawaiian time, when Fuchida signaled his aircraft to begin the attack. ¹⁷
2.2 GOVERNANCE LAYERS AND INTEROPERABILITY

In this section, we apply the 25 deficiencies to a fictitious world model of public safety and emergency response interoperability. We stress that this World Interoperability Model is entirely fictitious and is not meant to represent any specific organizational entities, agencies, departments of government, regions, nations, etc. This model is established exclusively to:

- Depict worst-case leaders and bureaucracies that plan and sustain public safety and emergency response organizations at all governance levels
- Present a worst-case picture of information-sharing deficiencies – primarily caused by failures of leadership to plan interoperability, governance, resources, approach, architecture, performance, and acceptance.
- Establish an “as-is” world environment for public safety and emergency response IT/communication systems as a baseline for the application of best practices in the development of IT/communications systems.

Figure 1 shows several levels of governance that impact the world’s responder-receiver organizations responsible for public safety and emergency response. In our fictitious model, all governance levels and their associated stakeholders produce overlapping responsibilities (Deficiency #1) and conflicts between disciplines (Deficiency #20) in preparedness and response. These deficiencies are inevitable in this often uncoordinated plethora of human organizations with overlapping goals and objectives.

We purposely place the local level at the highest position in the hierarchy because it is the local-level responders-receivers that must compensate in initiative and self-sacrifice because of failed interoperability. We also assume that there are multiple public safety and emergency response disciplines at each governance level of the world model below the local agency level. The leaders of each of these agencies are assumed to:

FIGURE 1. LEVELS OF GOVERNANCE
• Intensely protect and minimize dissemination of their information well beyond the protection of criminal or health care (Deficiency #3).

• Confuse personal connections with the leadership of other agencies as interoperability (Deficiency #21).

• Garner and protect available resources, and mask any personal or organizational inability to perform optimally (Deficiency #20).

• Not know what processes to use to seek and remedy the Pearl Harbor deficiencies in their own organizations (Deficiency #24).

Governance leaders overseeing one or more agencies at all levels

• Believe that nothing significant could happen in their jurisdiction (Deficiency #7) and cannot envision what could happen (Deficiency #10) or instead focus on what might happen versus what could happen (Deficiency #18).

• Don’t have the time (Deficiency #22) to verify adequate information sharing (Deficiency #17) among the organizations within their jurisdiction.

• Don’t know how to determine the necessary information sharing (Deficiency #15) or what processes to follow to improve any apparent needs (Deficiency #24).

Most importantly, and for reasons which have nothing to do with their prowess as leaders or planners, they simply have not had the professional exposure, much less the training or practical experience, in the application of best practices for identifying deficiencies and systematically eliminating them (Deficiency #24). No matter how effective their leadership, we assume they are not trained as practicing professionals in the fields of project management (PM), organizational development and effectiveness (OD&E), cost/benefit analysis (CBA), business case analysis (BCA), enterprise architecture (EA), systems engineering and integration (SE&I), funding strategy, training and exercises, etc. Nevertheless, these best practices should be used to mitigate and eliminate the deficiencies leading to interoperability failures.

In our World Interoperability Model, the 25 deficiencies negatively impact the preparedness and response of responders/receivers at all governance layers (e.g., local, county, state, national, and multinational). We will assume that national leaders and planners have sweeping oversight over critical aspects of public safety and emergency response policy. National-level leaders control national resources, including the radio spectrum and financial resources identified for public safety and emergency response organizations. However, these people are furthest removed from understanding the multilevel deficiencies at and below the local governance layer where most responders/receivers operate. Ironically, these national leaders are also furthest removed from the responder/receivers and their information-sharing deficiencies than all
other governance layers of the world model, but they have the greatest potential impact on interoperability, governance, resources, and approach.

In our fictitious worst-case world model, these national leaders

- Assume that someone in the governance levels at or below their national level is addressing the problem using best practices (Deficiency #2).
- Have no direct sustained experience in the public safety and emergency response domain (Deficiency #3).
- Have not inspected capabilities at all governance levels to understand how they will – or will not – interoperate in crisis (Deficiency #4).
- Lack understanding of the depth of information-sharing deficiencies within their national jurisdiction (Deficiency #15).
- Have no knowledge of the best practices needed to improve the status quo (Deficiency #24) on a nationwide level.
- Believe that inadequate information-sharing – if it in fact exists – is someone else’s problem at other governance levels (Deficiency #25).

In our fictitious world model, those judging the performance of ineffective planners cannot assess their employees’ performance, both because they have no experience or metrics themselves and because they insist there are many more important problems to address (Deficiency #22). Public safety nevertheless remains a government’s highest priority – at least theoretically – in our fictitious world model, but is not systematically supported or improved at the national level in any country.

In this regard, the greatest contribution these national leaders could make would be to systematically develop specific national – and multinational – mandatory interoperability Architecture standards (operational and system of systems). However, the national political understanding of these deficiencies, and the will and skill to mitigate or eliminate them, does not exist in any nation within our fictitious world model. As a result, none of the leaders responsible for national public safety and emergency response architecture either know how to plan to achieve interoperability, or if they do know, their efforts will neither be supported nor sustained by the governance or with the resources needed to achieve it. As a result, they, at best, succumb to Deficiency #20 and protect themselves and their organization from assertions that they have not done their job effectively in our fictitious world model. For this reason, information-sharing failures are either unknown or made invisible – no one asks the obvious questions.

In general, multiple agencies at all governance layers have overlapping IT/communication systems in certain geopolitical areas of the country where they have a role, such as border crossings, major urban areas, etc. No properly planned and
documented sharing of actionable information exists on a permanent basis among these agencies, and when they do, are limited to voice only on cached portable radios. Figure 2 shows the many IT/communication-system islands nationwide, including the addition of many overlapping national systems. These national systems include military, paramilitary, and intelligence organizations that electronically connect to many of the same networks and airwaves. However, these networks are isolated and remain incapable of optimally sharing information due to their purposed stand-alone design and lack of detailed cross-agency information-sharing architecture. Thin lines of information sharing not depicted in the figure, representing some minimal capability forced upon these organizations by absolute necessity, are not promoted for maximum benefit to the public. Again, in our fictitious world model, the 25 deficiencies are alive and well – and no systematic application of best practices have been applied to improve preparedness and response.

**FIGURE 2. IT/COMMUNICATIONS ISLANDS AT THE NATIONAL LEVEL.**

At the multinational level in our fictitious World Interoperability Model, responders-receivers from all governance levels must interoperate across international boundaries. Here, the lack of a national information-sharing architecture and associated gaps ensures the Pearl Harbor deficiencies will dominate preparedness and response, even in the most advanced countries. These gaps are exaggerated by language and cultural differences, adding additional layers of potential interoperability failure. Finally, international police and paramilitary forces – such as those operated by international
organizations – offer yet again another layer of potential deficiencies. Of course, the officials who oversee the aggregation and use of these forces are both the furthest removed from the responders-receivers on scene and least knowledgeable of their ingrained interoperability problems in the affected countries.

Figure 3 shows our IT/communication information-sharing architecture in the World Interoperability Model as a menagerie of disconnected islands with no overlapping capability, save for thin-line diplomatic communications and international commercial telephone networks. Military organizations – such as NATO and others – offer a means of transnational communications, if not information sharing, but capacity and civil use, for our purposes, are assumed to be negligible.

FIGURE 3. WORLD INTEROPERABILITY ARCHITECTURE.
2.3 OTHER FACTORS

2.3.1 BUREAUCRACIES IN OUR WORLD MODEL

Although elected or appointed leaders are inherently transient, many government layers maintain administrative bureaucracies with personnel that remain in place for many years. In our fictitious world model, therefore, we will assume that these bureaucrats maintain their positions for life – or until some form of retirement – irrespective of the success they achieve in bringing about true interoperability. Job titles may change, organizations may be merged or reorganized, but the same individuals remain in place for decades. In our fictitious world model, these individuals most assuredly maintain the same deficiencies inherent in their abilities and jurisdictions. They prevent innovators in their organizations from making effective change, using their internal political leverage to stop such innovators as their success would question the role of the long-term, in-place bureaucrat and their public service job. This state of affairs was arguably irrelevant before CBRNE WMDs and automatic weapons – but today, the Pearl Harbor ghosts haunt every unprepared community in every jurisdiction, region, and nation.

In these cases, the Pearl Harbor deficiencies remain endemic to a system that maintains these bureaucrats in place independent of their performance, such as #9 Attitude, #15 Insight, #20 Protectiveness, #21 Relationships, #22 Priority, and #24 Improvement. Again, this world model is meant only as an unrealistic worst-case representation of the world’s interoperability status. Failure to consider this worst-case scenario itself suggests Deficiency #10 Imagination – namely, “worst-case scenarios not included in preparedness and response planning.” As is well known, if the people, processes, and tools remain the same, and we simply call them something different, then the fundamental deficiencies will remain and the public will remain at risk, perhaps at greater risk. Thus, in our fictitious World Interoperability Model, the in-place bureaucracies are not capable of changing the status quo – and there is no accountability.

2.3.2 CONSULTANTS IN OUR WORLD MODEL

In our fictitious world model, leaders and planners hire consultants to effectively outsource the study their interoperability problems. In this world model, these consultants are assumed to have little or no direct experience in public safety and emergency response interoperability, much like their sponsors. They provide high-level plans or observations already well known by responders-receivers – translating the status quo into terms understandable to the sponsoring organization, or most frequently, lend support to decisions already taken by their sponsoring organization. However, we assume that the scope of these efforts is limited to radio interoperability and not the information-sharing deficiencies at the heart of interoperability failures. As with the bureaucrats, these planning consultants do not follow systematic best practices. In our fictitious world model, popular consultants are used extensively by agencies that need to show progress towards interoperability. For many reasons, we assume these
consultants know nothing of the Pearl Harbor deficiencies and are not fundamentally capable of systematically planning their mitigation or elimination. Even if competent, the in-place bureaucrats will tie their continued employment to consultant recommendations that retain the status quo.

2.3.3 VENDORS IN OUR WORLD MODEL

In our fictitious world model, the IT/communication systems planned and implemented by independent agencies achieve what they were designed to do, and interoperability as defined in this paper is not a design consideration, much less a source of detailed requirements. More importantly, each vendor contributing products to IT/communication systems at any governance level seeks to maximize the sale of their own products – a natural assumption in our fictitious world model. In this regard, it is in the apparent best interest of any vendor – in their stovepipe solution to the interoperability problem – to have all public safety and emergency response organizations buy products from them alone. As it has been since the most fundamental beginnings of radio and telecommunications, this motivation is a natural deterrent to interoperability. We assume that national leaders are not capable, or if capable are prevented for fear of adverse commercial impact, of mandating such critically important standards for civilian public safety and emergency response. Our fictitious world model assumes the public remains at risk for perceived commercial benefit. In fact, the majority of vendors would benefit from national standards – and there is precedent for mandatory IT/communication standards in the military domain. Although there are examples of national and international initiatives to standardize technology and mandate its use, this same treatment has not been applied with the same speed, resources, and commitment for information sharing in the civilian public safety and emergency response community as for the world’s warfighters. In our fictitious World Interoperability Model, we add the ranks of our responders-receivers to the warfighters and seek equal priority for national commitment.

2.4 WORLD INTEROPERABILITY MODEL

The World Interoperability Model multidimensional planning problem is depicted in Figure 4, in which each layer of governance, combined with the intra-agency deficiencies, is shown mapped against the six elements of interoperability. The resulting three dimensions of interoperability deficiencies produce a large matrix of potential interoperability failures which have been apparent for...
many decades – but for which no overarching approach has been put forward to mitigate and eliminate them. In our fictitious world model, failed interoperability planning by those in leadership roles at all governance levels forces the responders-receivers to demonstrate increasing initiative and personal sacrifice.

In our world model, we have an important dichotomy in leadership between the levels of governance. At the local governance level, the leadership is closest geographically and politically to those they support. These local responder-receiver organizations have the fewest resources of other governance layers, the responsibility of immediate response to incidents, and yet remain vulnerable to the 25 deficiencies. To address these deficiencies, they will need the planning capabilities and unified architecture from regional- and national-level governance layers, but they don’t exist. They are not capable or empowered to define architecture for the region or the nation by themselves and, therefore, need direction and common architecture provided to them from the regional and national governance levels. This is their dilemma: greatest real responsibility, least Approach and Resource capability (Deficiency #25).

At the other extreme, there are national- and international-level officials with no public safety or emergency response experience. They too are subject to the 25 deficiencies, and also do not know how to mitigate or perhaps even recognize the core interoperability problem: the lack of a best-practices-derived information-sharing architecture. As has been emphasized to this point, the tragic consequences of failed information sharing will continue worldwide until intelligent, informed, directed, and properly funded processes are employed to achieve true interoperability for our public safety and emergency response responder-receiver warfighters. Following proper processes, IT/communication systems can be designed to mitigate the 25 deficiencies and achieve interoperability.

3. ACHIEVING INTEROPERABILITY

3.1 PHILOSOPHY

The fundamental philosophy required to achieve interoperability worldwide is both “top-down” and “bottom-up.” Multinational and national authorities must define the overarching operational and system architecture, while responders-receivers themselves, at all governance levels, determine their information-sharing architecture. The national level provides the architecture and process. The responders-receivers “plug into” that architecture and employ the best-practiced-derived processes, but fill the associated requirements templates with their specific information-sharing requirements. The architecture and processes are designed to mitigate and eliminate the 25 deficiencies by a national collection of experienced practitioners.

3.2 MULTINATIONAL FRAMEWORK

Interoperability planning nation-to-nation must be linked, so information portals in one country are “linkable” under appropriate conditions to those of another (much like
today’s international air traffic control confederation of IT/communication systems). Autonomous multinational entities or confederations (e.g., the European Union) provide the best format for multinational information sharing tailored uniquely to each geopolitical region. In our fictitious world model, individual nations within a multinational entity are assumed to agree on a pair-wise, independent, nation-to-nation, information-sharing profile (i.e., specific event-based information sharing) within this entity. At worst, an entity is composed of a single (isolated) nation. Planning frameworks must be established at the multinational entity and national levels, but all information-sharing requirements must come directly from the responder-receiver organizations themselves, using standardized template formats.

3.3 NATIONAL-LEVEL FRAMEWORK

Interoperable planning is essential to developing interoperable systems at all levels of governance, certainly within a single nation. For this reason, standardized frameworks for governance structures, Resource planning, Approach best practices, Operational and System Architecture, Performance metrics, and Acceptance methods must be established at each national governance level. Standard structure and terminology must be employed to allow translatable, nation-to-nation co-planning. Having established a common framework for interoperability planning, it is next essential to have the information-sharing needs determined using this framework directly from the responders-receivers at all governance levels within each nation.

**Governance framework.** Each multinational entity and each contributing nation must establish a governance board with standard charter that (i) defines representative membership processes from different national regions; (ii) describes how decision-making and voting will be conducted; (iii) provides a standard set of committees addressing each interoperability element in the nation. Best practices for these national (and sub-national) interoperability governance boards will be developed from OD&E best practices (e.g., strategic planning and change management). Existing national governance bodies would be adequate at the onset of nationwide planning if proven effective.

**Resources framework.** Standard national methods for funding interoperability planning are documented and shared, with nations utilizing existing methods if proven effective. Spectrum, grants, and other resources must be tied to the use of national architecture and specific best practices to develop the information-sharing architecture, rather than general interoperability principles.

**Approach framework.** A standard set of integrated processes and associated interoperable tools will be employed to support planning of interoperable operational and system architecture. The process will include PM, OD&E (including knowledge management), CBA, BCA, EA, SE&I, funding strategy, training and exercises, etc., and flowcharts of when to employ which templates to be used to guide planners in developing the national operational and system architecture.
Architecture framework. The people, processes, and systems that constitute:

- **Operational architecture**, including doctrine, concept of operations (CONOPS), and common operating frameworks, such as the Incident Command System (ICS), SOPs, memoranda of understanding (MOUs), training and exercises, etc.

- **System architecture.** The IT/communications infrastructure, interface protocols, metadata, terminology, etc. that must be defined at the multinational and national levels to provide a common “bus” for interoperability at all higher levels of governance among responder-receiver organizations. Since information-sharing between operations centers (OPCENs) at all governance layers is critical, a model for the “to-be” system architecture for an OPCEN might appear as in Figure 5, where specific interfaces to other OPCENS are identified for interoperability.

Performance framework. Standard quantitative interoperability metrics, such as information timeliness and accuracy, completeness, etc.

Acceptance framework. Methods to build and enhance responder-receiver and government leader/planner support for nationwide interoperability planning initiatives. This framework uses tools from OD&E, such as the collaborative focus group, to bring disparate public safety and emergency response planners together and build consensus.
on the other interoperability elements above. In addition, these techniques would be used in collecting information-sharing requirements from all responder-receiver organizations.

Of course, these frameworks would be applicable for establishing interoperability plans at all other governance levels, including the local level, as well as within all responder-receiver organizations.

### 3.4 RESPONDER-RECEIVER INFORMATION-SHARING ARCHITECTURE REQUIREMENTS

The responder-receiver organizations at all levels of governance must provide their information-sharing requirements according to the standard formats developed by the national-level frameworks. At least five basic formats – or architectural views\(^\text{18}\) – are required to capture the necessary information-sharing requirements. Figure 6 shows the types of information required for both the as-is and best-practices-based should-be configuration of the IT/communications system architecture for public safety and emergency response. The information is captured for both the as-is and should-be information-sharing architectural framework views as follows:

- **Operational views**
  - Operational Activity Model – a flowchart of processes and information flows
  - Connectivity Description – depiction of nodes, information exchanges, and activities
  - Information Exchange Requirements – information exchange details supporting operational needs

- **System views**
  - System Interface Description – systems nodes, systems, system items, and their interconnections
  - Systems Communications Description – communication link descriptions

In addition, other useful architectural views important in simulating the processes and information flows needed to plan their implementation include:

- **Operational views**
  - Operational Event-Trace – traces actions in a scenario or sequence of events

- **System views**
  - Systems Event-Trace Description – identifies system-specific refinements of critical sequences of events described in the operational view

By collecting the key as-is and should-be operational architecture views for public safety and emergency response tasks and activities into a single analysis tool, simulations of the operational processes and system architecture can be performed. This “gap
analysis” identifies the specific activity-based information-sharing needs of each organization from which an information-sharing architecture can be defined and diagrammed for all governance layers. Once designed in an iterative process, MOUs would be established, and SOPs developed (perhaps automated) for developed for tailored sharing of actionable information to mitigate or eliminate the 25 Pearl Harbor deficiencies.

In addition, IT/communication system architecture gaps would be identified to meet operational needs, versus the failed practice of “buy first, plan later.” Best-practice plans are then developed to move to the “should-be” configuration through a series of “to-be” procurement programs as necessary. These plans are designed to achieve and sustain the essential capabilities (including telecommunications) to meet the operational information-sharing needs. This approach is appropriate for responder-receiver organizations at each governance level in the World Interoperability Model, with information inputs and outputs to and from, respectively, all other relevant organizations at all governance levels.

![Diagram of information-sharing architecture views](image)

**FIGURE 6. COLLAGE OF INFORMATION-SHARING ARCHITURE VIEWS**

4. SUMMARY

This paper has shown that the obstacles to achieving true interoperability for public safety and emergency response responders-receivers in a fictitious World Interoperability Model are the same as the deficiencies in American leadership found
after the Japanese attack on Oahu in December 1941. In reality, these deficiencies are not only endemic to the United States in 1941, but represent failures in leadership worldwide that strongly impact our public safety and emergency response responders-receivers. These deficiencies are present in many day-to-day tragedies, and all major ones, with names like Titanic (1912), Lusitania (1915), Poland (1939), Coventry (1940), Russia (1941), Bastogne (1944), Hiroshima (1945), Beirut (1983), 9-11 (2001), Madrid (2004), Tsunami (2004), Katrina (2005), Mumbai (2008), next (200?) …

In our world of CBRNE WMDs and automatic weapons used by fanatic killers of innocents, properly designed information-sharing architecture could have

- Prevented these surprises and avoided the catastrophic consequences.
- Speeded early detection and alerting, enhanced situational awareness and coordinated command in managing response, and ensured more rapid and complete recovery in unpreventable disasters.

Information-sharing architecture must be developed and institutionalized at all levels of governance. In this regard, the 25 deficiencies serve as a checklist for current system evaluation and future system enhancement or development. It is a complex and difficult issue, all the more reason to get started now in building a resilient society.19. Ironically, our public safety and emergency response organizations and the communities they protect are information islands, much like the organizations in Washington, D.C., and on the Island of Oahu at 0749 December 7, 1941. Will we remain asleep to the warnings and ignore the danger as they did?

ACKNOWLEDGEMENTS

The author sincerely thanks Mr. Pat Lanthier, Founder & Chair of the Emergency Communications Leadership & Innovation Center (eCLIC) of the Wireless Communications Alliance (WCA), for the opportunity to develop this paper and present at the 2009 Pacific Telecommunications Conference. I thank Mr. Christopher P. ‘Jake’ Jacobson for his best practices in information-architecture development. I also want to thank Ms. Suzanne J. MacBain of Newton, Massachusetts, for her excellent editing of the draft manuscript, both of this paper and the parent book manuscript. I also wish to thank Ms. Rozlyn A. Reece and Ms. Mary F. Cates for their professional review and my collaborator Peter J. Rosamilia for orchestrating completion of the work.

REFERENCES

ENDNOTES

1. This paper was derived from Desourdis, Robert I., et al, Achieving Interoperability in Public Safety and Emergency Response IT/Communication Systems, Artech House, Boston, forthcoming.
2. For example, hospital and community shelter personnel.
10. Ibid.
15. Cmdr. Mitsuo Fuchida led the first-wave air attack on Pearl Harbor.