MTR 05W0000065

MITRE TECHNICAL REPORT

Application of a Readiness Model for Multi-Agency Interaction

September 2005

P. Kathie Sowell
Ann E. Reedy
Mimi Kidest Hailegiorghis

Sponsor: The MITRE Corporation
Dept. No.: V410 **Project No.:** 19MSR022-CA

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation. Work performed under MITRE Sponsored Research (MSR) Project Multi-Agency Architecture Planning Framework.

MITRE
Center for Enterprise Modernization
McLean, Virginia

MITRE Department Approval:

Anne R. Cady, V010

MITRE Project Approval:

Dr. Kenneth C. Hoffman, V410

Abstract

In the post-9/11 world, the private sector and multiple government organizations at the Federal, State, and local levels need to work more closely together than before to prevent and solve problems, including terrorist actions.

The Readiness Model is a tool to help in planning, training for, and executing actions that require the participation of multiple organizations with interacting command and control structures. The model provides a logic for assessing the degree to which organizations need to work together to get a given job done and the degree to which they are prepared to do so. Readiness Model analysis involves the discipline and artifacts of Enterprise Architecture, using an Operations-Centric representation that describes the specific activities performed, the services required, and decision responsibilities to perform the mission.

This paper illustrates the application of the Readiness Model to a scenario and architecture that involve a hypothetical biological and radiological threat.

Key Words: Collaboration, Enterprise Architecture, Interaction, Maturity Model, Multi-Agency, Readiness Analysis, Services

Acknowledgments

The Readiness Model applied in this paper is treated more thoroughly in MITRE Technical Report (MTR050000012), *A Readiness Model for Multi-Agency Interaction* [1]. This paper is a companion to that Technical Report and shows how the Readiness Model can be applied to a given scenario. The basic scenario used for this purpose was developed under an IR&D project to illustrate an environment for executable architectures. The authors wish to acknowledge Tom Pawlowski, Ken Hoffman, David Payne, Kangmin Zheng, and Meghan Williams for providing that scenario. The authors further acknowledge that they have made several modifications to the original scenario in order to emphasize important aspects of the readiness model.

The Readiness Model and this application were developed under MITRE Sponsored Research (MSR) on Multi-Agency Architectures.

Table of Contents

1 THE READINESS MODEL 1

2 CRITERIA FOR ATTAINING EACH LEVEL OF INTERACTION 3

3 COMPONENTS OF READINESS MODEL ANALYSIS 5

4 USING THE READINESS MODEL IN ARCHITECTURAL ANALYSIS 7

5 EXAMPLE APPLICATION OF THE READINESS MODEL 9

6 CONCLUSIONS 25

7 COMPLETE EXCHANGE MATRIX FOR THE RESPONSE TO BIOLOGICAL/RADIOLOGICAL TERRORIST ATTACK ARCHITECTURE 27

8 REFERENCES 35

List of Figures

FIGURE 1. THE FULL READINESS MODEL FOR MULTI-AGENCY INTERACTION....2
FIGURE 2. CRITERIA FOR ACHIEVING LEVEL 1 INTERACTION: OPERATION COORDINATION....3
FIGURE 3. CRITERIA FOR ACHIEVING LEVEL 2 INTERACTION: OPERATION COOPERATION....4
FIGURE 4. CRITERIA FOR ACHIEVING LEVEL 3 INTERACTION: OPERATION COLLABORATION....4
FIGURE 5. RECOMMENDED ARTIFACTS TO INCLUDE IN THE OPERATIONS-CENTRIC ARCHITECTURE....5
FIGURE 6. ACTIVITY MODEL OF THE STEPS IN USING THE READINESS MODEL....7
FIGURE 7. SCENARIO PROBLEM STATEMENT: RESPONSE TO BIOLOGICAL/RADIOLOGICAL TERRORIST ATTACK....9
FIGURE 8. OPERATIONAL CONCEPT: RESPONSE TO BIOLOGICAL/RADIOLOGICAL TERRORIST ATTACK....10
FIGURE 9. OPERATIONS-CENTRIC ACTIVITY MODEL: RESPONSE TO BIOLOGICAL/RADIOLOGICAL TERRORIST ATTACK....11
FIGURE 10A. EVENT TRACE MODEL: RESPONSE TO BIOLOGICAL/RADIOLOGICAL TERRORIST ATTACK....12
FIGURE 11. NODE CONNECTION MODEL: RESPONSE TO BIOLOGICAL/RADIOLOGICAL TERRORIST ATTACK....15
FIGURE 12. SYSTEM INTERFACE MODEL: RESPONSE TO BIOLOGICAL/RADIOLOGICAL TERRORIST ATTACK....18
FIGURE 13. BUSINESS ACTIVITIES TO INFORMATION SERVICES MATRIX....19
FIGURE 14. PROFILE OF THE REQUIRED INTERACTION BETWEEN THE PORT REGION AUTHORITIES HEADQUARTERS EMERGENCY OPERATIONS CENTER AND THE STATE POLICE COMMAND CENTER IN THE BIOLOGICAL/RADIOLOGICAL OPERATION....20
FIGURE 15. PROFILE OF THE REQUIRED INTERACTION BETWEEN THE PORT REGION AUTHORITIES HEADQUARTERS EMERGENCY OPERATIONS CENTER AND THE FIRST RESPONDERS IN THE BIOLOGICAL/RADIOLOGICAL OPERATION....21
FIGURE 16. PROFILE OF THE REQUIRED INTERACTION BETWEEN THE PORT REGION AUTHORITIES HEADQUARTERS EMERGENCY OPERATIONS CENTER AND NATIONAL CIVIL SECURITY IN THE BIOLOGICAL/RADIOLOGICAL OPERATION....22
FIGURE 17. OVERALL INTERACTION PROFILE FOR THE BIOLOGICAL/RADIOLOGICAL RESPONSE OPERATION....23

List of Tables

TABLE 1. EXTRACT FROM THE OV-3 EXCHANGE MODEL: RESPONSE TO BIOLOGICAL/RADIOLOGICAL TERRORIST ATTACK 16
TABLE 2. COMPLETE EXCHANGE MATRIX FOR THE RESPONSE TO BIOLOGICAL/RADIOLOGICAL TERRORIST THREAT ARCHITECTURE 28

1 The Readiness Model

In the post-9/11 world, it has become increasingly clear that multiple organizations need to work more closely together than ever before to prevent and solve problems. This need is recognized today, as evidenced by the proliferation of terms like "horizontal fusion," "horizontal integration," "vertical integration," and "interoperability." Working together is especially critical in preventing and addressing terrorism, because many Federal, State, and local governments and the private sector need to share information and perform anti-terrorism activities in sync. They also need to plan and train together.

A Readiness Model provides an objective means of measuring how well organizations are positioned to work together to accomplish specific missions. This paper focuses on an example application of a Readiness Model but provides only a brief overview of the model itself. For more details of the Readiness Model see MITRE Technical Report (MTR050000012), *A Readiness Model for Multi-Agency Interaction* [1].

The characteristic that the Readiness Model measures is termed "interaction." "Interaction" was chosen instead of "interoperability," "cooperation," "integration," or other such terms because each of these terms has specific connotations for different communities of interest, and because the Readiness Model really addresses all of these. Each participating organization has other jobs to do besides the Multi-Agency one being examined, but how well each organization performs those other jobs is not the concern here. In fact, how well each organization does its own part of the Multi-Agency job is not even the main concern. The main concern in a Multi-Agency operation is how well the participants *perform together*. This measure of how well a group is positioned to accomplish the operation's goals is the Readiness Profile of the group. Figure 1 shows the full Readiness Model for Multi-Agency Interaction. Note that each level of interaction is described in terms of four descriptors: Governance, Activities, Data, and Technology. The gray text in parentheses under Governance indicates that common funding is a goal, but is not usually the case today.

Level 3 Collaboration			
Governance	**Activities**	**Data**	**Technology**
▪ A single set of goals is set ▪ Overall Multi-Agency operation is governed by a single person or governing body who is accountable and has command authority (e.g., Chairman of the U. S. Chief Information Officers' Council, or a Joint Task Force) ▪ An integrated set of performance measures is analyzed and enforced by the governing body ▪ All involved agencies train together for the whole operation ▪ (Funding for most activities comes from a common budgeting action and source)	▪ Most critical activities are performed collectively by Communities of Interest whose members come from more than one agency (i.e., no single agency can perform those activities effectively alone)	▪ In most cases, data exchange between agencies is critical for accomplishing the activities ▪ Asynchronous status reports are not enough; most activities cannot be performed without real time exchange of information; common data ▪ Before-the-fact and real time planning	▪ Most core systems and applications (sensors, weapons, analysis software, etc.) need to be interoperable; some common applications ▪ Comm systems need to interoperate ▪ Synchronous, session-based virtual meetings needed to create, edit, review multi-media information ▪ Most intranets linked across agency boundaries ▪ Core services are shared
Level 2 Cooperation			
Governance	**Activities**	**Data**	**Technology**
▪ Agencies have different goals ▪ Actions are governed independently (i.e., no single person or body is accountable for overall success) ▪ Some cross-agency performance measures, but analyzed/enforced separately ▪ Selected agencies train together for some common activities of the operation ▪ (Some funding (for the common activities comes from a common budgeting action and source)	▪ At least one activity is performed collectively by Communities of Interest whose members are drawn from more than one agency (i.e., no single agency can perform this activity(ies) effectively alone)	▪ In some cases, data exchange between agencies is critical for accomplishing the activities ▪ Asynchronous status reports are not enough; some activities cannot be performed without real time exchange of information beyond telephone or conversations (e.g., multi-media, video, etc.) ▪ Before-the-fact and real time planning	▪ Some core systems and applications (sensors, weapons, analysis software, etc.) need to be interoperable ▪ Comm systems need to interoperate ▪ Synchronous, session-based virtual meetings needed to create, edit, review multi-media information ▪ Some linked intranets across agency boundaries ▪ Some support services are shared
Level 1 Coordination			
Governance	**Activities**	**Data**	**Technology**
▪ Agencies have different goals ▪ Participants and actions are governed independently (i.e., no single person or agency is accountable for overall success) ▪ Single-agency performance measures ▪ Agencies train separately ▪ Agencies plan separately ▪ Agencies are budgeted and funded separately for all their actions	▪ Results of activities of some participating agencies influence the actions of other agencies (i.e., agencies need to know what other agencies are doing, but don't need to perform activities together)r	▪ Data exchange between agencies is desirable but not critical ▪ Asynchronous status reports, near-real time warnings ▪ Before-the-fact planning (synchronous and asynchronous)	▪ Core systems and applications (sensors, weapons, analysis software, etc.) can be non-interoperable ▪ Comm systems need to interoperate ▪ Asynchronous info exchange tools are sufficient for most needs; some low-tech synchronous info exchange (e.g., sneaker net, conversation, telephone) ▪ Single-agency intranets ▪ Single-agency services

Figure 1. The Full Readiness Model for Multi-Agency Interaction

2 Criteria for Attaining Each Level of Interaction

Readiness Criteria are a set of questions about the organizations that participate in a given operation and about the operation itself. Figures 2 through 4 show criteria for each descriptor within each interaction level.

Governance	Activities	Data	Technology
• Have a governance structure and process been formalized for each agency? • Are the structure and process understood within the agency? • Have mission measures of success been defined within the agency? • Has the governance body identified other missions/operations that may affect the current mission? • Is the governing body for each agency aware of the training schedule and content of other agencies?	• Have the critical activities of each agency been identified and described? • Are the activities understood within each agency? • Has each agency identified other agencies' activities that might affect its own activities?	• Has each agency defined relevant terms for its own use? • Are the relevant terms understood the same way by all participants within the agency who need to exchange information? • Have the cross-agency participants who need to exchange information for pre-operation coordination been identified?	• Have the comm systems and networks involved in the operation been identified for each agency? • Is there at least one interoperable comm system at each end of the information exchange? • Have the core systems used by each agency been identified?

Figure 2. Criteria for Achieving Level 1 Interaction: Operation Coordination

Governance	Activities	Data	Technology
• Have measures of success been consistently defined across missions and agencies? • Do the agencies involved in common activities train together for those activities?	• Have the activities that require agency-to-agency interaction been identified? • Have the activities that require agency-to-agency interaction been defined at the appropriate level of detail across all relevant agencies?	• Have relevant terms been defined in a consistent way in all participating agencies? • Have the agencies that need to exchange information been identified? • Has the data that needs to be exchanged been identified and described? e.g, • Content • Who needs it • Who supplies it • How often needed • Security Classification	• Have the comm systems and networks involved in the information exchange been identified? • Have the core systems involved in the information exchange been identified? • Are these comm and core systems and networks interoperable? (e.g., has a Levels of Information Systems Interoperability analysis been done that shows they can exchange data?)

Figure 3. Criteria for Achieving Level 2 Interaction: Operation Cooperation

Governance	Activities	Data	Technology
• Have a governance structure and process been formalized for the overall operation? • Has a single person or governing body been put in place who is accountable and has command authority? • Do all agencies participate in operation planning? • Have measures of success been defined for the overall operation? • Are the governance and measures of success understood consistently across participating agencies? • Do all agencies train together, including those agencies that do not require direct interaction in the operation?	• Do all agencies understand and agree on the set of activities that require cross-agency interaction?	• Has the format of the data that needs to be exchanged been determined?	• Are the systems and applications involved in cross-agency interaction used the same way in multiple agencies, i.e., are the rules and policies compatible across agencies?

Figure 4. Criteria for Achieving Level 3 Interaction: Operation Collaboration

3 Components of Readiness Model Analysis

The main components of the Readiness Model are an Operations-Centric Architecture and various interaction profiles. The interaction profiles identify the readiness characteristics of critical agency pairs, of individual agencies, and of the operation as a whole, and are therefore termed Readiness Profiles. The Readiness Profiles are described in Section 5, in the course of describing an application of the Readiness Model to an example operation.

The Operations-Centric Architecture consists of various types of models, or artifacts. Figure 5 lists the artifacts and maps each artifact to the descriptors for which it provides information. Artifacts in bold type are those that are most important for Readiness Model use. Most of the artifacts shown in the figure are the artifacts specified in the Department of Defense Architecture Framework (DODAF), version 1.0 [2].

Descriptors	Governance	Activities	Data	Technology
Architecture Artifacts	▪ Mission and Vision Statements ▪ Overview and Summary Descriptions ▪ **Operational Concept Documentation** ▪ Organizational Relationships Charts ▪ **Activity Models**	▪ **Operational Concept Documentation** ▪ **Activity Models** ▪ **Event Trace Models** ▪ **Node Connection Models** ▪ **Exchange Matrices** ▪ **Business Activities to Information Services Matrix**	▪ Data Models ▪ **Node Connection Models** ▪ **Exchange Matrices**	▪ System Inventories ▪ **System Interface Descriptions** ▪ System Functionality Models ▪ **Business Activities to Information Services Matrix**

Figure 5. Recommended Artifacts to Include in the Operations-Centric Architecture

4 Using the Readiness Model in Architectural Analysis

Figure 6 illustrates the steps for applying the readiness model to analysis of an operation. In addition to the steps, the figure indicates some of the artifacts that result from the steps.

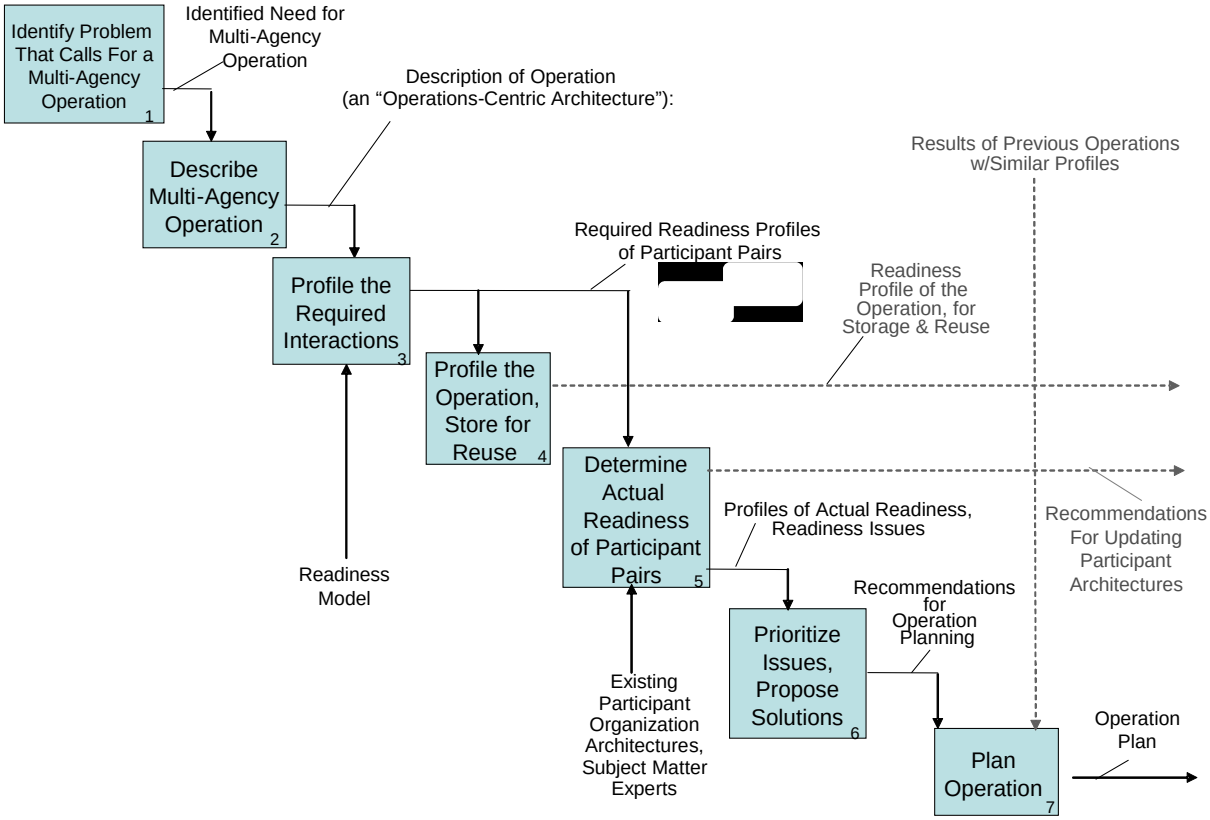

Figure 6. Activity Model of the Steps in Using the Readiness Model

5 Example Application of the Readiness Model

Each of the Readiness Model steps is described in the following example case, beginning with the Problem Statement (see Figure 7).

Step 1: Identify a Problem Area That Calls for a Multi-Agency Operation

Detecting biologically hazardous material imported into the U.S. via shipping containers and preventing its transportation and dispersal within the U.S. is the overall mission of the example operation. Various echelons of threat detection and response organizations must interact to detect problems, track the material, and coordinate response actions in this mission. For this example, a specific scenario is used to demonstrate an instance of this mission. Figure 7 states the focused problem statement for this scenario.

Scenario Problem Statement:
Terrorists have obtained biologically hazardous radioactive material, have offloaded it at a U.S. port, and are transporting it on a commercial truck. Various echelons of threat response organizations must interact to track the material and coordinate response actions.

Figure 7. Scenario Problem Statement:
Response to Biological/Radiological Terrorist Attack

Step 2: Describe the Multi-Agency Operation

The scenario selected for this application of the Readiness Model is a hypothetical one. Its purpose is only to illustrate the Readiness Model, not to represent reality. In some cases, capabilities that do not currently exist are shown, such as the video conferencing capabilities that most local agencies and States do not have.

The operation description is in the form of an Operations-Centric Architecture [3]. In this example case, the Operations-Centric Architecture consists of an Operational Concept Description (Figure 8), an Event Trace Model (scenario sequence, Figure 9), an Activity Model (Figure 10), a Node Connection Model, (Figure 11), an Exchange Matrix (Table 1), a System Interface Description (Figure 13), and a Business Activities to Information Services Matrix (Figure 13).

Figure 8 provides an overview of the concept for this architecture. It illustrates the geographical location (hypothetical “Adamstown” and “Jeffersonville”), the detection of radioactive material (in the Cobalt 60 Blood Irradiator which contains Co60, a radioactive material), and the range of agencies that participate in detection, tracking, and coordination of the response.

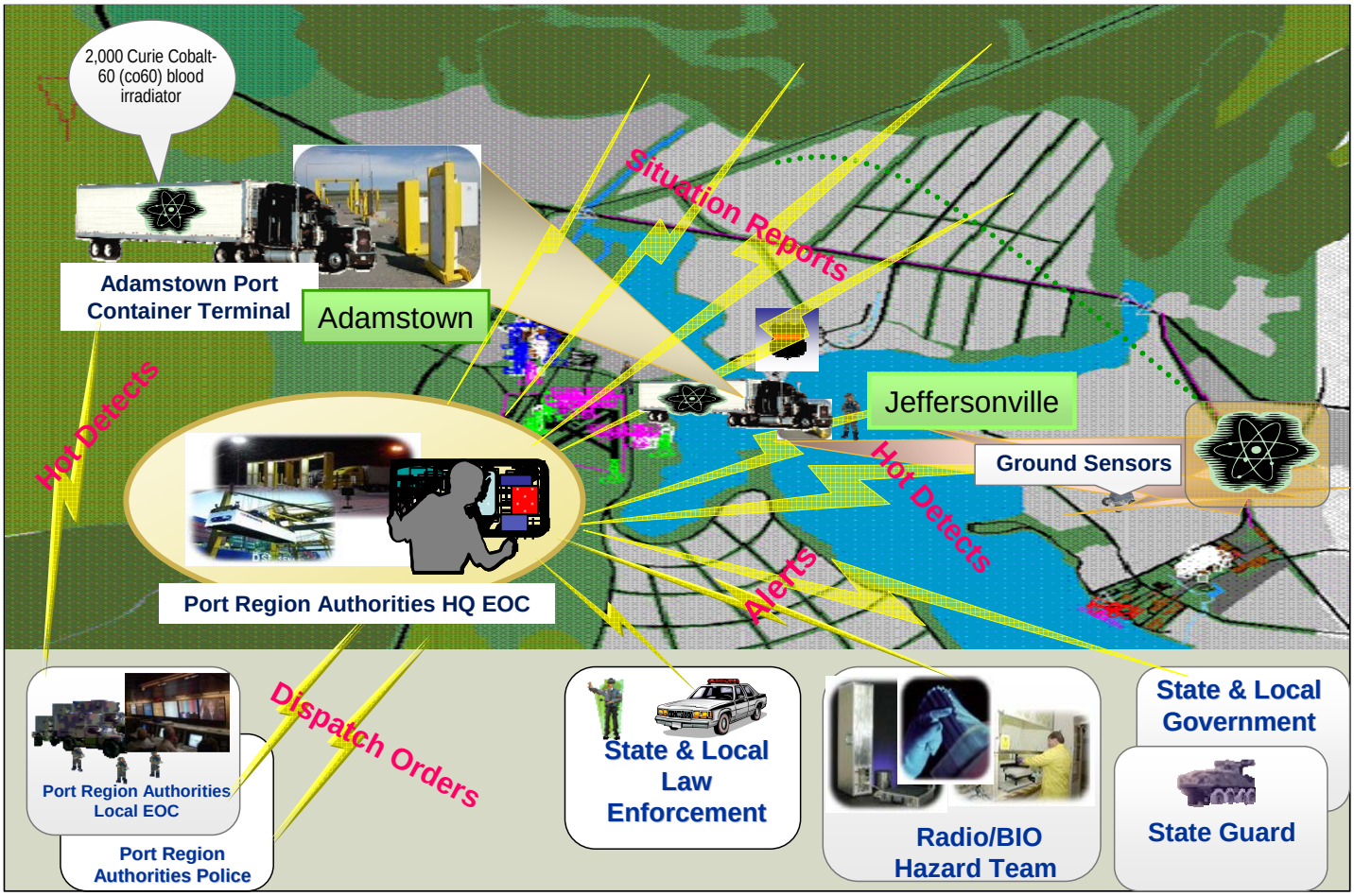

Figure 8. Operational Concept: Response to Biological/Radiological Terrorist Attack

The Activity Model in Figure 9 describes the high-level actions that occur in the course of detecting the radioactive threat, tracking its progress, responding to the threat, and recovering after the event. The decomposition of each activity box is indicated by bullets within each box. The organizations that participate in performing each of the activities are indicated by the arrows entering the bottom of each activity.

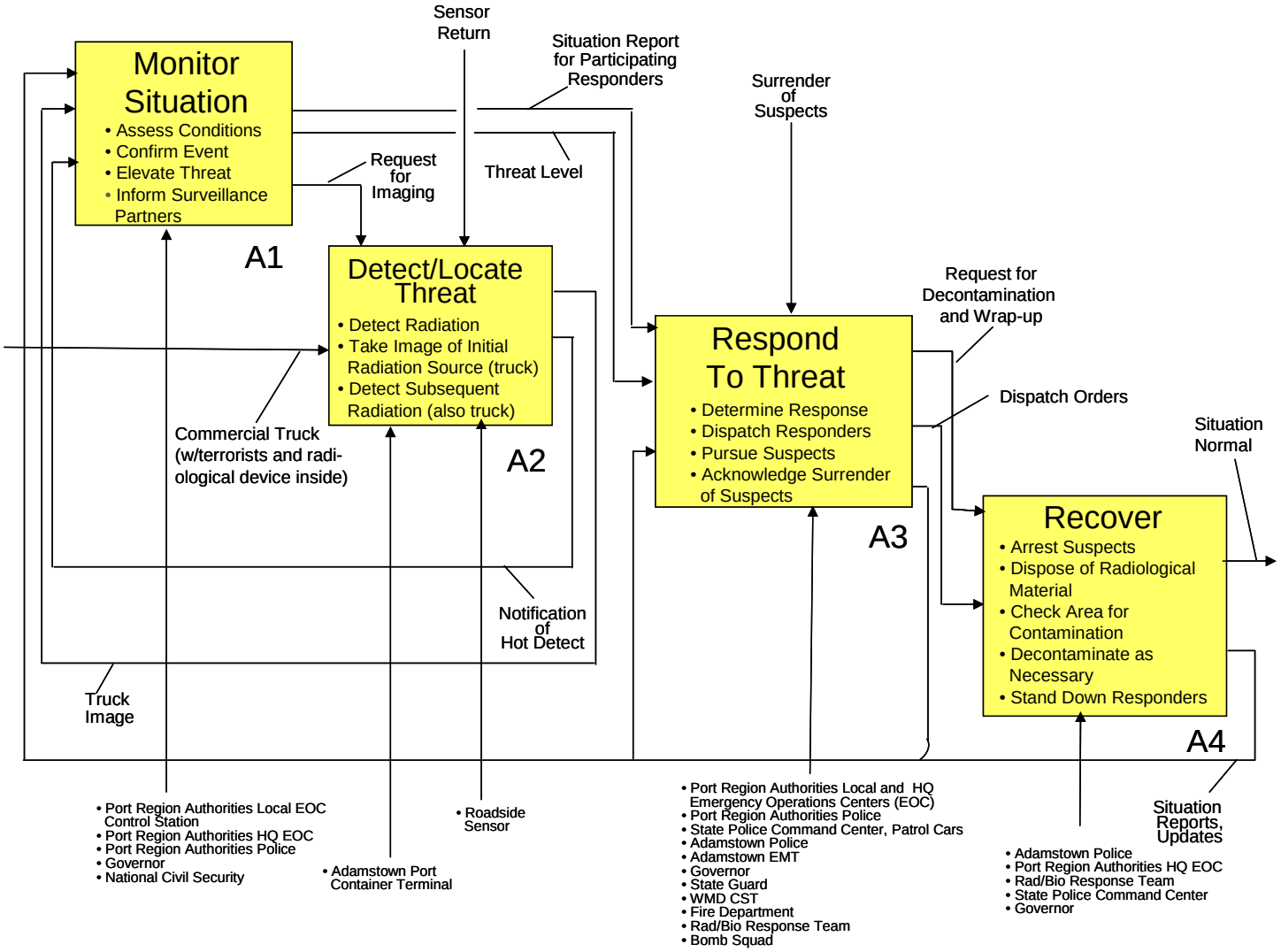

Figure 9. Operations-Centric Activity Model: Response to Biological/Radiological Terrorist Attack

Figures 10a and 10b represent the Event Trace Model for this scenario, which describes a time-sequenced unfolding of the scenario.

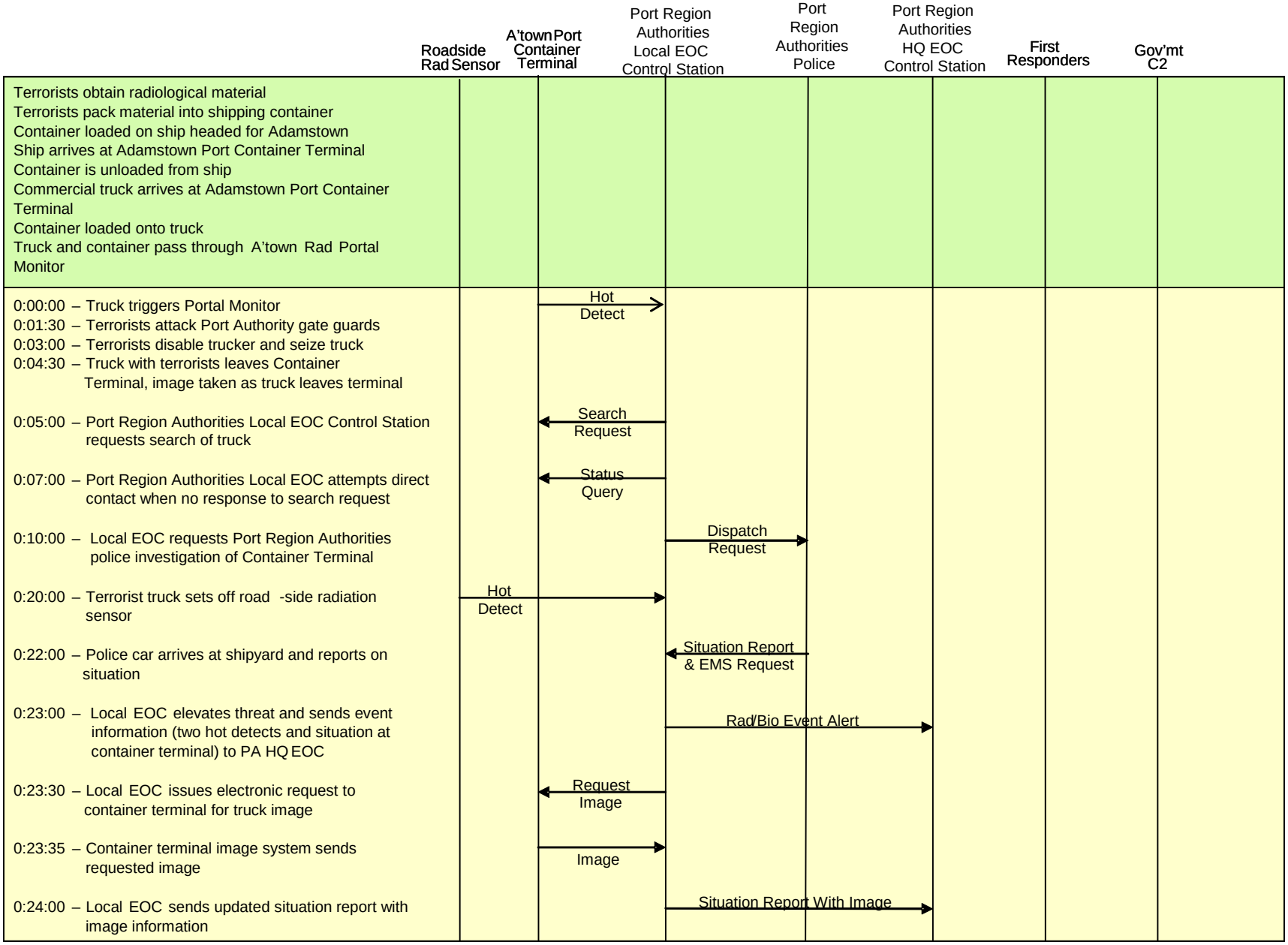

Figure 10a. Event Trace Model: Response to Biological/Radiological Terrorist Attack

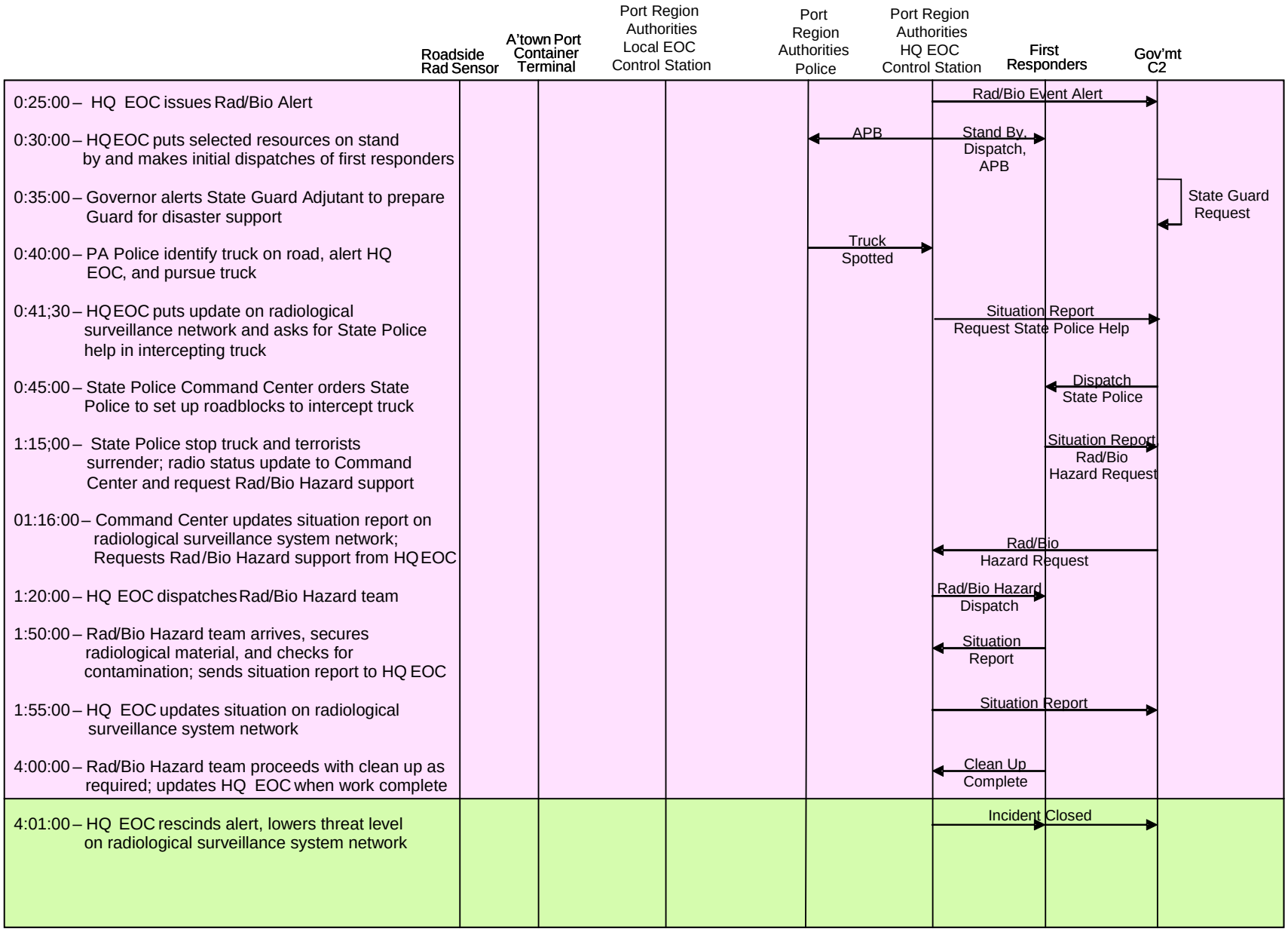

Figure 10b. Event Trace Model: Response to Biological/Radiological Terrorist Attack (concluded)

Time moves from top to bottom, along with the events. Across the top of the figure are the organizations that perform the activities shown in the Activity Model; arrows indicate information exchange. Color bands are for ease of reading, and indicate phases of the scenario. Some of the agencies are aggregations, e.g., "Government Command and Control." These agencies include the State Police Command Center, the Governor, National Civil Security, and the State Guard Adjutant.

Figure 11, the Node Connection Model, shows information exchanges. "NL" means "needline" and indicates information providers/consumers. The participating agencies are termed "nodes." These nodes are largely the same as the agencies shown in the Activity Model and the Event Trace Model, with some of the aggregations broken out into individual agency nodes. Two additional nodes, the terrorist cell and the container ship, are shown inside dotted lines. The dotted lines indicate that these nodes are "external nodes," that is nodes that are included for context but that do not perform activities from the Activity Model. The activities (from the Activity Model) that are performed by each node are listed on the model in blue text. The activity number is listed instead of the activity name.

It is important to note that the needlines do not indicate point-to-point connections; they only indicate which nodes provide information and which nodes receive it. Needlines 1-3 are different from the others in that they indicate exchange of a physical object (the radioactive material itself) rather than information. This is a non-standard tailoring of the Node Connection Model, used in this example to allow the Node Connection Model to tell a more complete story.

Table 1 shows an extract from the Exchange Matrix for this scenario. In an Exchange Matrix, the needlines from the Node Connection Model are detailed to show individual information exchanges and some of the important characteristics of the exchanges. Appendix A contains the entire Exchange Matrix for this example architecture.

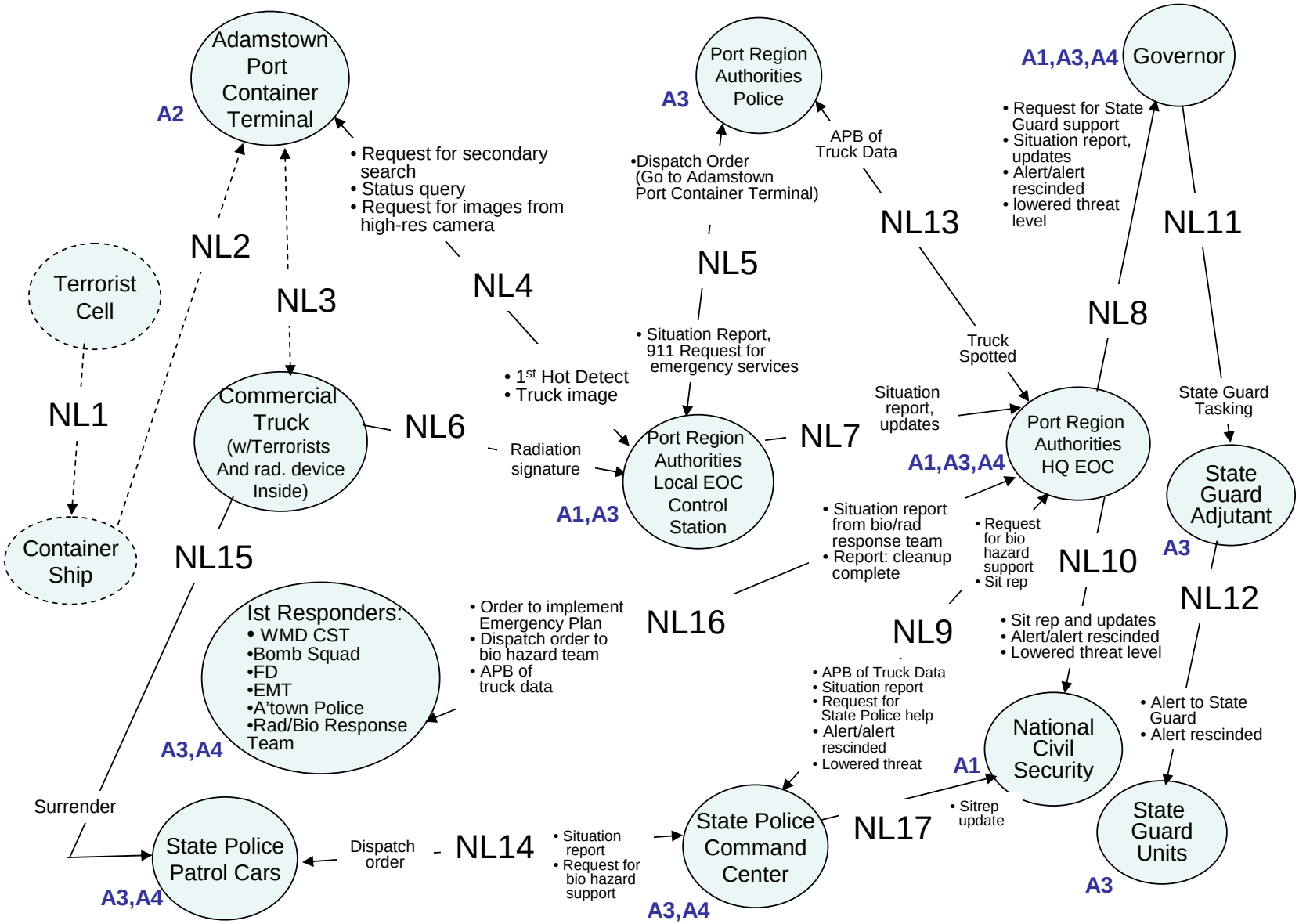

Figure 11. Node Connection Model: Response to Biological/Radiological Terrorist Attack

Table 1. Extract from the OV-3 Exchange Model: Response to Biological/Radiological Terrorist Attack

Needline Number	Information Exchange ID	Content	Media (Voice, Data, Text, …)	Producing Node	Producing Activity	Consuming Node	Consuming Activity	Triggering Event	Security (High, Medium, Low)	Criticality (1 – 3)
1		Co60 Blood Irradiator	Physical Object	Terrorist Cell (external node)	N/A	Container Ship	N/A	Ship Loaded	N/A	N/A
2		Co60 Blood Irradiator	Physical Object	Container Ship	N/A	Adamstown Port Container Terminal	N/A	Ship Unloaded	N/A	N/A
3	**3a**	Co60 Blood Irradiator	Physical Object	Adamstown Port Container Terminal	N/A	Commercial Truck	N/A	Truck Loaded with Container	N/A	N/A

The System Interface Model in Figure 12 overlays identifiers of hardware and software systems onto the Node Connection Model. That is, this model shows what systems the agencies use to implement the logical information exchanges shown in the Node Connection Model.

In some cases, these systems are physical systems that provide information, such as "High-Resolution Video Camera," "First Radiation Sensor," and "Sensor Analysis Workstation." In other cases, what is shown is a system service that needs to be provided, without an identification of the actual system that provides it, such as "Secure Video Conference." Because this scenario involves multi-agency coordination, Secure Video Conference provides much of the required capability. The Secure Video Conference includes services such as Collaboration, Security, and Directory Services. The Central Radiological Surveillance System is an intranet that also helps to provide the Collaboration and Security services. The blue boxes represent physical items that can be considered systems but do not provide information exchange.

In most cases, the nodes shown on this System Interface Model are the same nodes that were shown on the Node Connection Model, but with their hardware and software systems now identified. The one exception is the Roadside Radiation Sensor, shown in pink, which did not appear on the Node Connection Model because it is a system implementation detail not needed at the Node Connection Model level. Most of the system interfaces, abbreviated "SI," map one-to-one with the needlines, abbreviated "NL," of the Node Connection Model; however, there are a few exceptions: Needlines 1, 2, and 3 do not have corresponding system interfaces because the exchanges in these cases are physical objects, not information, and no automated systems are used; and system interfaces 6a and 6b collectively implement needline 6.

The Business Activities to Information Services Matrix is shown in Figure 13. This matrix explicitly identifies the needed information services and maps them to the business activities and services derived from the Activity Model. Each entry in the matrix identifies the system or systems from the System Interface Description that supplies the information service to a business activity. The systems are identified in the matrix by a code number specified in the supplied key, which follows the matrix. The Business Activities to Information Services Matrix provides an explicit link between the Activities and Technologies descriptors of the Readiness Model. The Co60 Blood Irradiator is not shown in the matrix because it is not a system that belongs to the agencies and doesn't participate in the collaboration that is the focus of the Readiness Model.

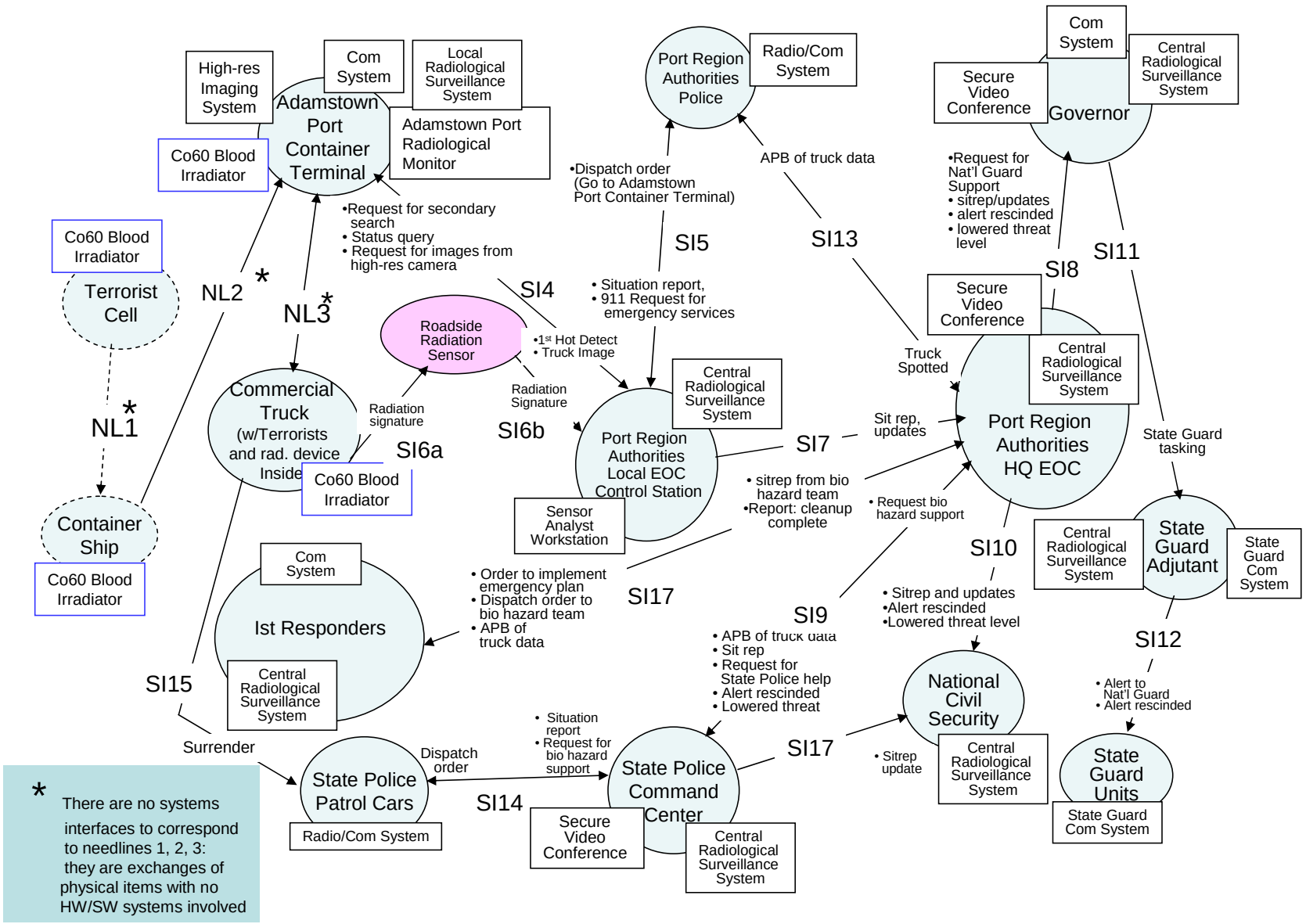

Figure 12. System Interface Model: Response to Biological/Radiological Terrorist Attack

Business Activities and Services/Information Services	Monitor Situation (A1)				Detect/Locate Threat (A2)			Respond to Threat (A3)				Recover (A4)				
	Assess Conditions	Confirm Event	Elevate Threat	Inform Partners	Detect Radiation	Take Image of Source	Detect Subsequent	Determine Response	Dispatch Responders	Pursue Suspects	Acknowledge Surrender	Arrest Suspects	Dispose of Material	Check for Contamination	Decontaminate as Necessary	Stand Down Responders
Detect Radiation					1		2									
Provide Images						3										
Share Threat Information with Surveillance Partners	4, 5	4	4	5, 10				4, 5	4, 5							4, 5, 10
Support Government C2 Ops Com				6, 10					6							10
Support Decision Analysis		7														
Provide Mobile and Voice Com	9			9 (back-up)				8, 9	8, 9	8	8				8	8, 9

System Key

1 Adamstown Port Radiological Monitor
2 Roadside Radiation Sensor
3 High Resolution Imaging System
4 Local Radiological Surveillance Network
5 Central Radiological Surveillance Network
6 Secure Video Conference
7 Sensor Analyst Workstation
8 Com System: Radio
9 Com System: Phone
10 State Guard Communications System

Figure 13. Business Activities to Information Services Matrix

Step 3: Profile the Required Interactions of Agency Pairs

Concentrating on the major, critical agency-pair interactions from the Node Connection Model, i.e., those that enable the critical activities from the Activity Model, the next step is to build a Readiness Profile of each interaction. These profiles show which agency pairs need to interact, and at what level they need to interact in terms of the four descriptors Governance, Activities, Data, and Technology (systems).

Figures 15, 16, and 17 illustrate three example agency interaction Readiness Profiles from this example case. The text boxes that point to the descriptor columns explain the rationale for the characterizations of the interaction levels for each descriptor.

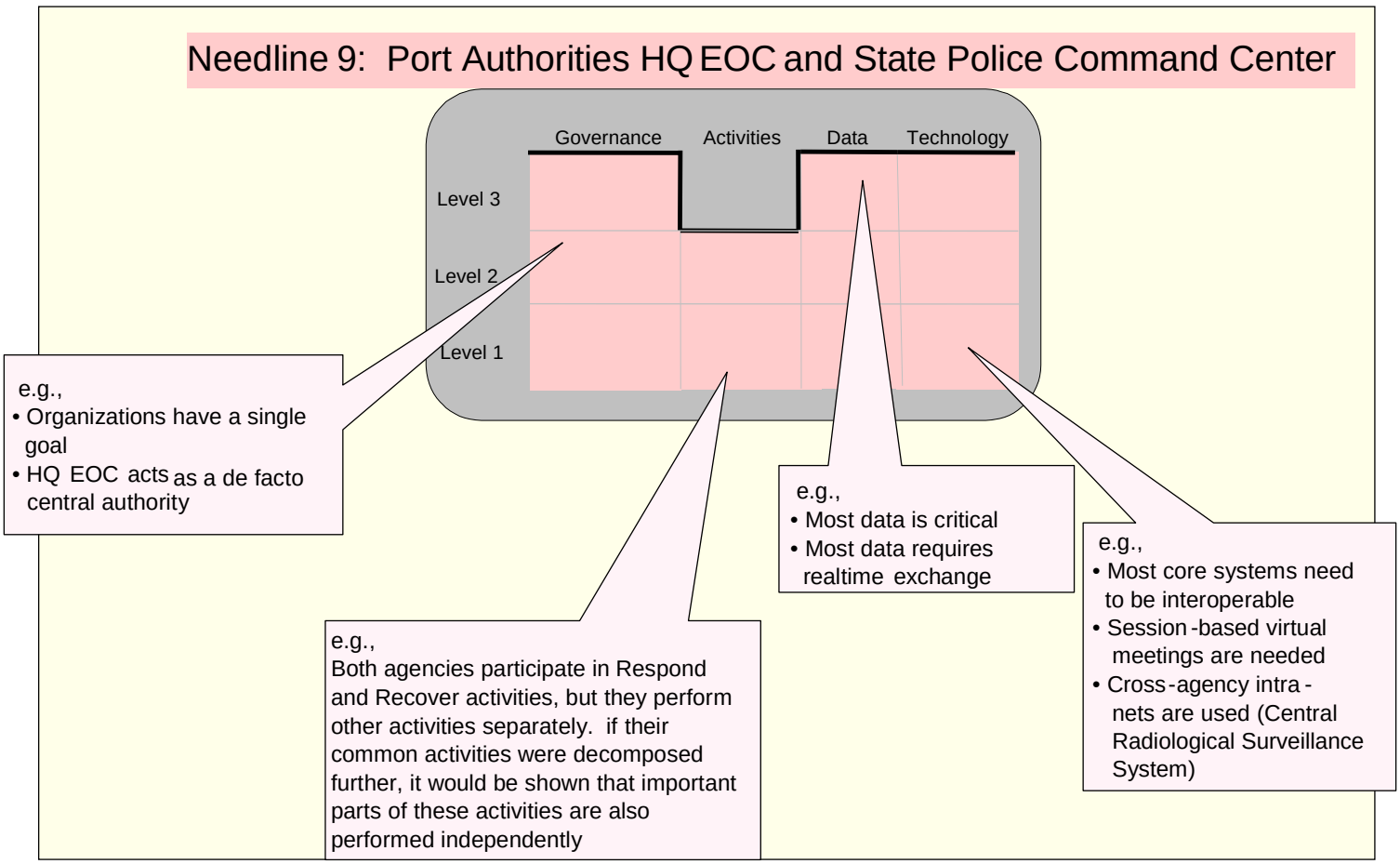

Figure 14. Profile of the Required Interaction between the Port Region Authorities Headquarters Emergency Operations Center and the State Police Command Center in the Biological/Radiological Operation

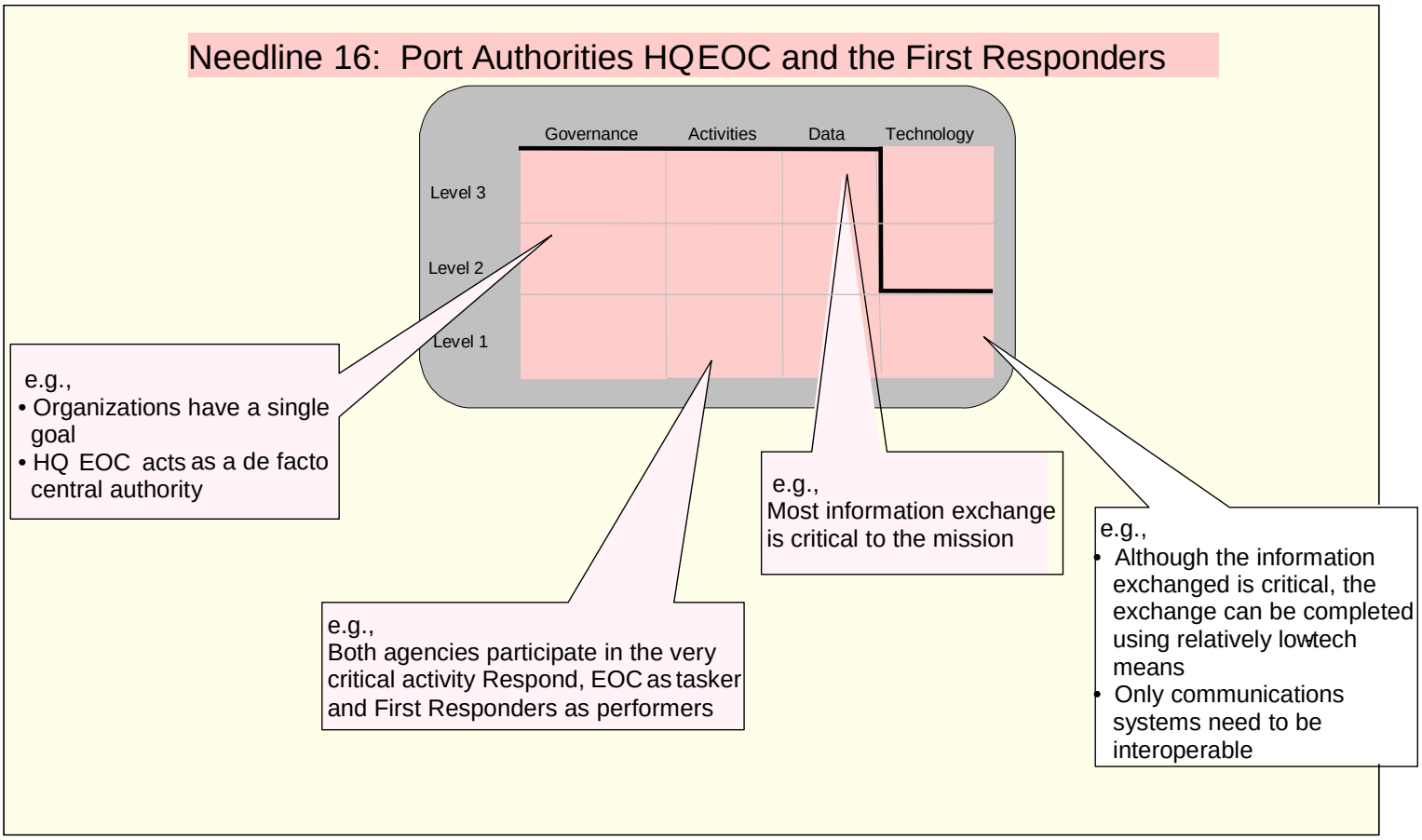

Figure 15. Profile of the Required Interaction between the Port Region Authorities Headquarters Emergency Operations Center and the First Responders in the Biological/Radiological Operation

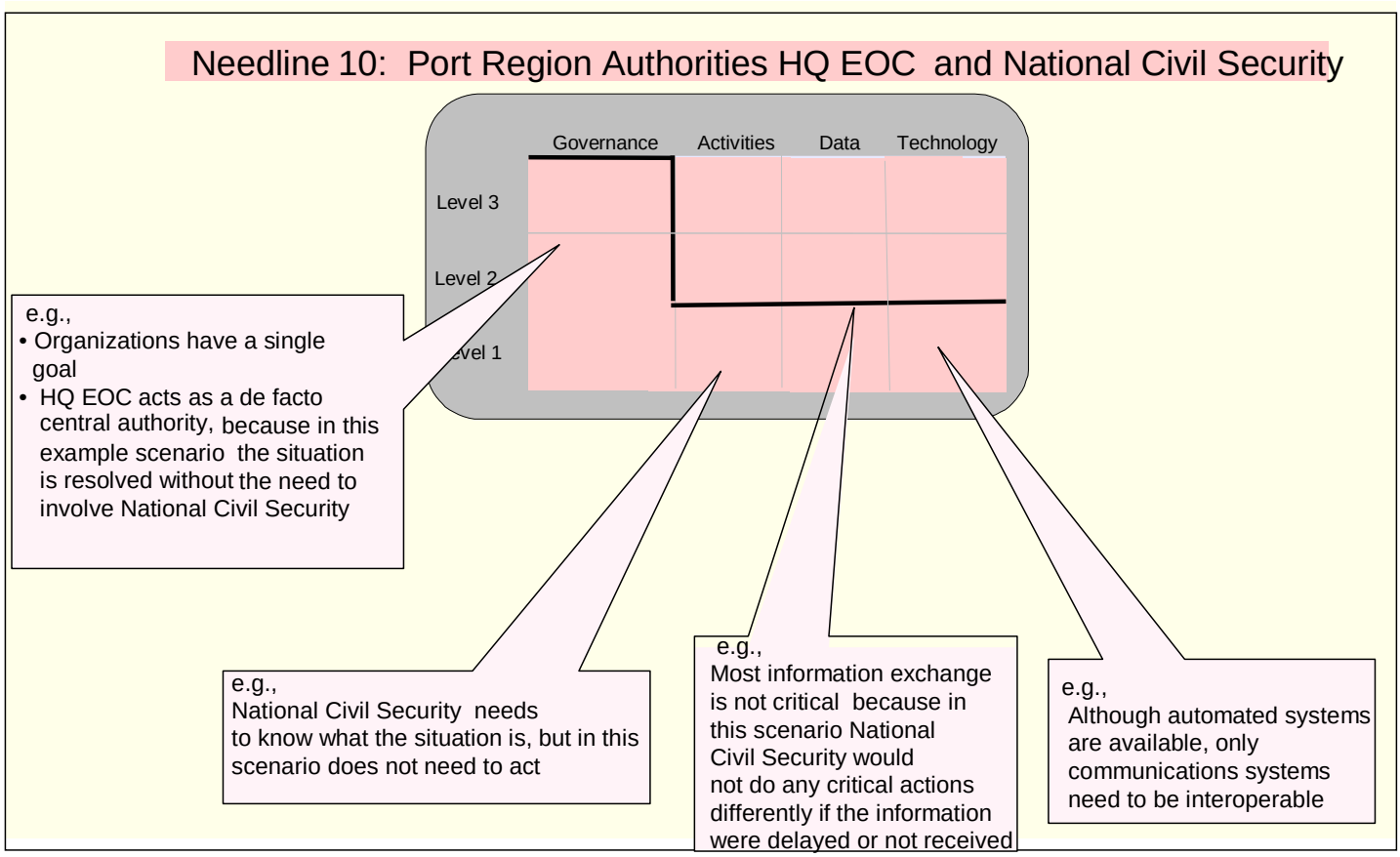

Figure 16. Profile of the Required Interaction between the Port Region Authorities Headquarters Emergency Operations Center and National Civil Security in the Biological/Radiological Operation

Step 4: Profile the Operation

Combining the individual agency-to-agency interaction Readiness Profiles results in a Readiness Profile of the operation as a whole (i.e., the most demanding interaction levels required between agency pairs in each of the descriptors). Figure 17 shows the overall operation Readiness Profile for the biological/radiological response operation. The figure indicates that the operation is a Level Three operation in all four descriptors, because each descriptor has at least one agency pair that operates at that level. For this example only three agency pairs are illustrated. However, the overall operation profile would be the same if all agency pairs were shown, because no agency pairs would be higher than Level Three unless the agencies were combined into a single organization, which does not apply to this operation.

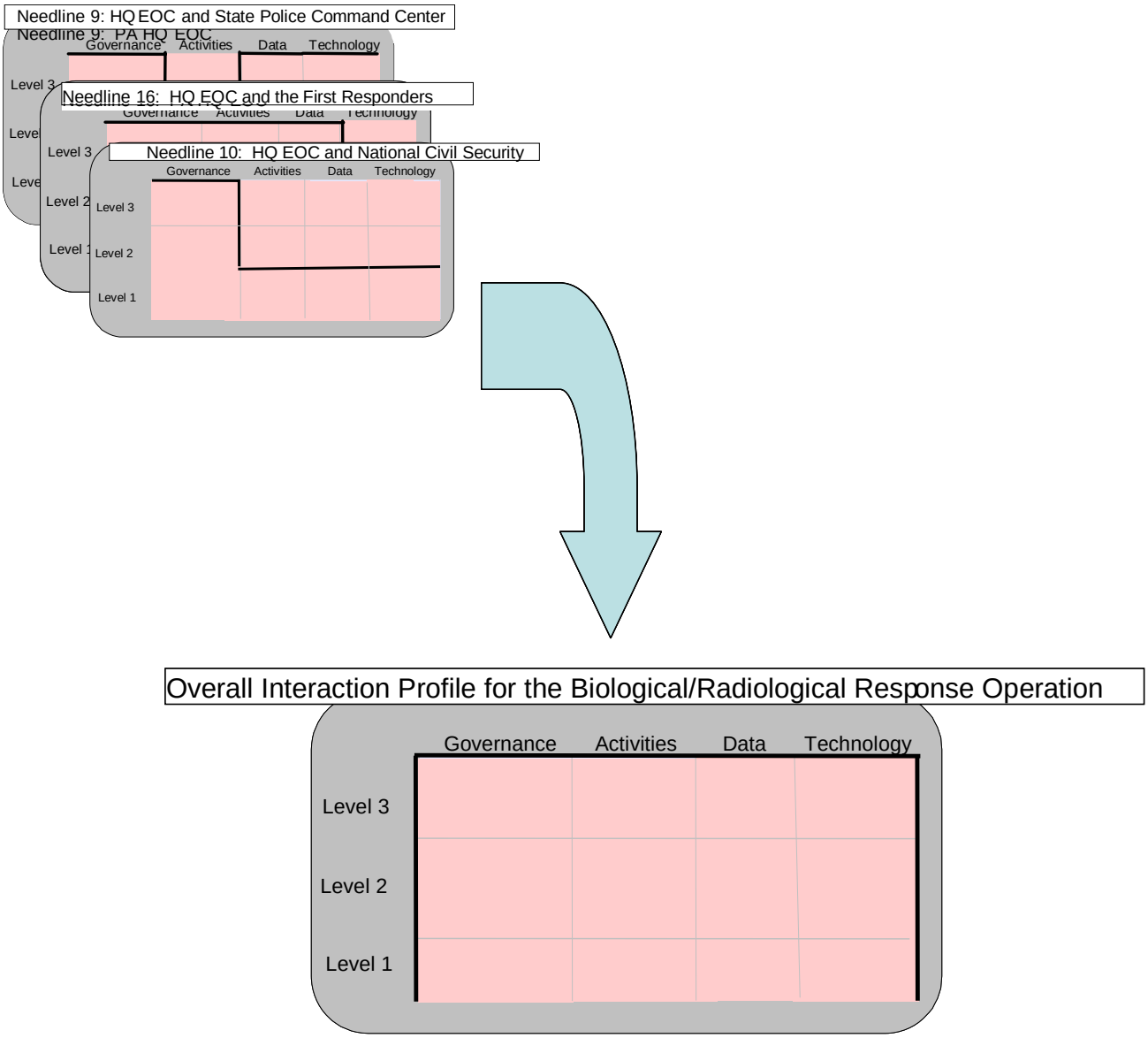

Figure 17. Overall Interaction Profile for the Biological/Radiological Response Operation

Step 5: Determine Readiness of Agency Pairs

This step answers the question "Are the agencies really ready to interact at the level that the operation requires?" One technique for addressing this question is to examine the enterprise architectures of the participating organizations, asking such questions as:

- Do the architectures exist?
- Do the architectures illustrate the activities and interactions that the operation requires?

- Do the interactions appear to satisfy the Governance, Activities, Data, and Technology requirements in the required Agency-to-Agency Readiness Profile?
- If not, where are the problems (in Governance, Activities, Data, Technology, a combination)?

The problems can be highlighted via an Actual Readiness Profile. Analysts should consult subject matter experts for clarification, and to obtain details not addressed in architectures. This step was not performed for this illustration of the Readiness Model.

Step 6: Prioritize Problems and Propose Solutions and Step 7 Plan Operation

These final steps were outside the scope of the effort and were not performed for this example application of the Readiness Model.

6 Conclusions

The Operations-Centric Executable Architecture concept deals with operations and technical systems performance [3]. The Readiness Model for Multi-Agency Interaction [1] is a valuable supplement to this methodology that deals specifically with the performance of the organizations involved. This paper has described an application of that Readiness Model to a specific scenario. The process of exercising the Readiness Model through application to a scenario has yielded some observations and lessons learned, which are described below.

First, the effort involved in developing an architecture from a scenario description should not be underestimated. In this effort, the authors began with a textual scenario that seemed straightforward at first. However, once we began to develop the architecture artifacts, we discovered that considerably more detail was necessary. The scenario events needed to be tied together with underlying information. For example, why did certain events occur, that is, what other events that were not called out in the scenario caused these events to occur? Which specific organizations performed the actions, and which subdivisions within those organizations? How was the information passed from organization to organization? Was the timing and sequencing in the scenario feasible? Which actions were supported by automation and which were purely manual? What services did the automated systems need to provide in order for the actions to take place? The authors believe that applying this level of discipline to a scenario description can be very valuable in testing scenarios for feasibility and can thus make scenarios more useful as a means for training and analysis.

Another observation is one that reinforces a statement in the Readiness Model paper: that an operation, or scenario, has a Readiness *Profile*, not just a single readiness *score*. The profile consists of scores for each of four descriptors (governance, activities, data, and technology) and each descriptor is important. The identification of decision-making responsibilities and activities across multiple organizations and command centers is a particularly important element of mission performance, along with the timing of these events over the course of the scenario. These governance aspects need to be given much more attention than was possible within the scope of this application.

Another observation is a caution. This paper illustrates the application of the Readiness Model to a single scenario. However, plans and acquisitions should not be made based on a single scenario. This is because the organizations involved will have different requirements based on different scenarios: when planning for organizational development, the group of all likely scenarios should be considered.

Finally, the authors believe that applying the Readiness Model to a set of scenarios can be a helpful tool for characterizing and validating the scenarios and for prioritizing them. A number of such sets of scenarios exist, for example the scenarios developed by the Department of Homeland Security [4]. Building an Operations-Centric Architecture for each of the scenarios would force a

level of discipline that would help to validate the scenarios. Then, attaching a Readiness Profile to each scenario via the Readiness Model would help to prioritize the scenarios for testing.

7 Complete Exchange Matrix for the Response to Biological/Radiological Terrorist Attack Architecture

The following pages contain the complete Exchange Matrix for the Response to Biological/Radiological Terrorist Attack architecture. In the matrix, individual needlines from the Node Connection Model have been decomposed into discrete information exchanges, where appropriate. Each information exchange is described in terms of the characteristics that are considered useful for the architecture's purpose.

Because the purpose of this architecture was to exercise the Readiness Model for Multi-Agency Interaction, the characteristics included in the Exchange Matrix are those that most affect interaction among operational nodes.

Table 2. Complete Exchange Matrix for the Response to Biological/Radiological Terrorist Threat Architecture

Needline Number	Information Exchange ID	Content	Media (Voice, Data, Text, …)	Producing Node	Producing Activity	Consuming Node	Consuming Activity	Triggering Event	Security (High, Medium, Low)	Criticality (1 – 3)
1		Co60 Blood Irradiator	Physical Object	Terrorist Cell (external node)	N/A	Container Ship	N/A	Ship Loaded	N/A	N/A
2		Co60 Blood Irradiator	Physical Object	Container Ship	N/A	Adamstown Port Container Terminal	N/A	Ship Unloaded	N/A	N/A
3	**3a**	Co60 Blood Irradiator	Physical Object	Adamstown Port Container Terminal	N/A	Commercial Truck	N/A	Truck Loaded with Container	N/A	N/A
	3b	Photons (picture taken)	Physical Object	Commercial Truck	N/A	Adamstown Port Container Terminal	N/A	Arrival of Truck at Sensor	N/A	N/A
4	**4a**	Detection Information (1st Hot Detect)	Data	Adamstown Port Container Terminal	A2	Port Region Authorities Local EOC Control Station	A1	Radiation Detected	H	1
	4b	Request for Secondary Search	Voice (Telephone)	Port Region Authorities Local EOC Control Station	A1	Adamstown Port Container Terminal	A1	Receipt of Detection Information	M	2
	4c	Status Query	Voice (Telephone)	Port Region Authorities Local EOC Control Station	A1	Adamstown Port Container Terminal	A1	Lack of Response within 2 min.	L	3

Needline Number	Information Exchange ID	Content	Media (Voice, Data, Text, …)	Producing Node	Producing Activity	Consuming Node	Consuming Activity	Triggering Event	Security (High, Medium, Low)	Criticality (1 – 3)
	4d	Request for Images from High Res Camera	Data	Port Region Authorities Local EOC Control Station	A1	Adamstown Port Container Terminal	A2	Receipt of 2nd Hot Detect	M	1
	4e	Truck Image	Imagery	Adamstown Port Container Terminal	A2	Port Region Authorities Local EOC Control Station	A1	Request for Image	H	1
5	**5a**	Dispatch Order	Voice (radio)	Port Region Authorities Local EOC Control Station	A3	Port Region Authorities Police	A3	Lack of Response to Status Query	H	1
	5b	Sit Rep, 911 request for emergency services	Voice (radio or telephone)	Port Region Authorities Police	A1	Port Region Authorities Local EOC Control Station	A3	Initial Assessment of Situation	M	2
6		Radiation Signature (2nd Hot Detect)	Data	Commercial Truck	N/A	Port Region Authorities Local EOC Control Station	A1	Radiation Detected	H	1
7		Situation Report	Data (Network)	Port Region Authorities Local EOC Control Station	A1	Port Region Authorities HQ EOC	A1	Receipt of 2nd Hot Detect/ Changed Situation	M	3

Needline Number	Information Exchange ID	Content	Media (Voice, Data, Text, …)	Producing Node	Producing Activity	Consuming Node	Consuming Activity	Triggering Event	Security (High, Medium, Low)	Criticality (1 – 3)
8	**8a**	Sit Rep Updates	Video	Port Region Authorities HQ EOC	A1	Governor	A1	Changed Situation	M	3
	8b	Alert/alert rescinded Threat level lowered	Data (Network)	Port Region Authorities HQ EOC	A4	Govenor	A1	Confirmation of Incident/ Change in Threat Level	L	1
	8c	Request State Guard Support	Video	Port Region Authorities HQ EOC	A3	Govenor	A1	Request of Alert	M	1
9	**9a**	APB for Truck: License plate number, Vehicle type and color, Number of occupants	Voice (radio)	Port Region Authorities HQ EOC	A3	Port Region Authorities Police	A3	Receipt of Truck Image Data	H	1
	9b	Situation Report	Data (Network)	Port Region Authorities HQ EOC	A1	State Police Command Center	A3	Change in Situation	M	3
	9c	Request for State Police Help	Voice (Telephone)	Port Region Authorities HQ EOC	A3	State Police Command Center	A3	Receipt of Truck Spotted Report	M	2
	9d	Situation Report	Data (Network)	State Police Command Center	A3	Port Region Authorities HQ EOC	A1	Change in Situation	M	3

Needline Number	Information Exchange ID	Content	Media (Voice, Data, Text, …)	Producing Node	Producing Activity	Consuming Node	Consuming Activity	Triggering Event	Security (High, Medium, Low)	Criticality (1 – 3)
	9e	Request for bio hazard support	Video	State Police Command Center	A3	Port Region Authorities HQ EOC	A3	Receipt of Request for Bio Hazard Support	H	1
	9f	Alert/alert rescinded Threat level lowered	Data (Network)	Port Region Authorities HQ EOC	A4	State Police Command Center	A4	Confirmation of Incident/ Change in Threat Level	L	1
10		Situation report Alert/alert rescinded Threat level lowered	Data (Network) Voice (Telephone backup)	Port Region Authorities HQ EOC	A1	National Civil Security	A1	Change in Situation Confirmation of Incident Change in Threat Level	L	1
11		State Guard Tasking (Deploy/ Stand down)	Voice (Telephone)	Governor	A3	State Guard Adjutant	A3 A4	Receipt of Alert	H	1
12	**12a**	Alert to State Guard	Voice (Telephone)	State Guard Adjutant	A1	State Guard Units	A1	Receipt of Alert	L	1
	12b	Alert Rescinded	Voice (Telephone)	State Guard Adjutant	A4	State Guard Units	A4	Receipt of Lowered Threat Level	H	1
13	**13a**	Report of truck spotted	Voice (Radio)	Port Region Authorities Police	A3	Port Region Authorities HQ EOC	A3	Visual Contact with Truck	M	1

Needline Number	Information Exchange ID	Content	Media (Voice, Data, Text, …)	Producing Node	Producing Activity	Consuming Node	Consuming Activity	Triggering Event	Security (High, Medium, Low)	Criticality (1 – 3)
	13b	APB for Truck: License plate number, Vehicle type and color, Number of occupants	Voice (Radio)	Port Region Authorities HQ EOC	A3	Port Region Authorities Police	A3	Receipt of Truck Image Data	H	1
14	**14a**	Dispatch Order	Voice (Radio)	State Police Command Center	A3	State Police Patrol Cars	A3	Receipt of Request for Assistance	H	1
	14b	Request for Bio Hazard Support	Voice (Radio)	State Police Patrol Cars	A3	State Police Command Center	A3	Surrender of Truck	H	1
	14c	Situation Report	Voice (Radio)	State Police Patrol Cars	A3	State Police Command Center	A3	Changed Situation	L	3
15		Surrender	Voice (Oral)	Commercial Truck	N/A (external node)	State Police Patrol Cars	A3	Decision of Terrorist to Surrender	L	1
16	**16a**	Order to Implement Emergency Plan	Voice (Radio/ Telephone) Data (Network)	Port Region Authorities HQ EOC	A3	1st Responders (all)	A3	Confirmation of Incident	H	1
	16b	Dispatch Order to Bio Hazard Team	Voice (Radio/ Telephone) Data (Network)	Port Region Authorities HQ EOC	A3	1st Responders (Bio Hazard Team)	A3	Receipt of Request for Bio Hazard Support	H	1
	16c	Situation Report, Report Clean Up Complete	Voice (Radio)	1st Responders (Bio Hazard Team)	A4	Port Region Authorities HQ EOC	A4	Assessment of Situation/ Completion of Clean Up	L	2

Needline Number	Information Exchange ID	Content	Media (Voice, Data, Text, …)	Producing Node	Producing Activity	Consuming Node	Consuming Activity	Triggering Event	Security (High, Medium, Low)	Criticality (1 – 3)
	16d	APB for Truck: License plate number, Vehicle type and color, Number of occupants	Voice (Radio)	Port Region Authorities HQ EOC	A1	1st Responders (all)	A3	Receipt of Truck Image Data	H	1
17		Situation Report Updates	Voice (Radio)	State Police Command Center	A3	National Civil Security	A1	Change in Situation	L	3

8 References

1. Sowell, P. K., February 2005, *A Readiness Model for Multi-Agency Interaction*, MTR050000012, The MITRE Corporation, McLean, VA.
2. www.http://osd.mil, Department of Defense Architecture Framework, version 1.0, 2003.
3. K. C. Hoffman, et al., Enterprise Business, Computing, and Information Services in a Multi-Agency Environment: A Case Study in Enterprise Architecture Engineering, IEEE Enterprise Distributed Objects Computing (EDOC) Conference, September 2005.
4. Department of Homeland Security, National Response Plan, December 2004, Washington, DC.