



Continuity Risk Toolkit

Support for Continuity Planning

January 2017



FEMA

This page is intentionally blank.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	iii
INTRODUCTION.....	1
Risk 101	1
Continuity Planning	4
CONCEPT OF OPERATIONS	5
Analysis Structure.....	5
ANALYSIS PHASES.....	7
Phase 1: Develop	7
Phase 2: Define	10
Phase 3: Assess	13
Phase 4: Enhance	16
METHODOLOGIES AND ANALYTIC TECHNIQUES	20
APPENDICES	24
Appendix A. Anticipatory Failure Determination.....	A-1
Appendix B. Benefit-Cost Analysis.....	B-1
Appendix C. Brainstorming Techniques.....	C-1
Appendix D. Cause and Effect Diagrams	D-1
Appendix E. Developing Factor-Based Models	E-1
Appendix F. Event Mapping	F-1
Appendix G. Event Tree Analysis	G-1
Appendix H. Expert-Opinion Elicitation Process	H-1
Appendix I. Failure Modes and Effects Analysis	I-1
Appendix J. Fault Tree Analysis.....	J-1
Appendix K. Hazard and Operability Analysis.....	K-1
Appendix L. Hierarchical Holographic Modeling.....	L-1
Appendix M. Influence Diagrams	M-1
Appendix N. Measurement of Intangibles	N-1
Appendix O. Preliminary Hazard Analysis.....	O-1
Appendix P. Premortem Analysis	P-1
Appendix Q. Problem Restatement and Issue Development	Q-1
Appendix R. Reliability Block Diagrams	R-1
Appendix S. Root Cause Analysis.....	S-1
Appendix T. Scoping a Risk Study.....	T-1
Appendix U. SIPOC Diagram.....	U-1
Appendix V. Sorting	V-1
Appendix W. System Description Methodology	W-1
Appendix X. Weighted Ranking	X-1
Appendix Y. Work Breakdown Structure.....	Y-1

THREAT AND HAZARD NETWORKS	Z-1
Appendix Z. Threat and Hazard Networks.....	Z-1
WORKSHEETS.....	AA-1
Appendix AA.Worksheets	AA-1
SUPPORTING APPENDICES.....	BB-1
Appendix BB.Glossary.....	BB-3
Appendix CC.References	CC-1

EXECUTIVE SUMMARY

The Continuity Risk Toolkit provides general information on risk and techniques that may be used to perform risk analysis. It serves as a continuity resource for stakeholders by providing reference material, information, and guidance intended to further develop and refine risk identification and determine the potential for all-hazard risks to affect the performance of essential functions and essential supporting activities (ESAs). It supports Federal Continuity Directives (FCDs) 1 and 2, which implement the requirements Presidential Policy Directive 40 (PPD-40), *National Continuity Policy*, and provide guidance to executive branch departments and agencies (D/As) on validation of Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs). A risk-based approach to business analysis informs decisions that sustain MEFs and PMEFs during all phases of a catastrophic emergency.

While the information in the Continuity Risk Toolkit focuses on methods for analyzing exposure to internal and external risks that have the potential to impact essential functions, other aspects of risk analysis (e.g., economic/financial, enterprise, security) may be essential for organizational-level vulnerability assessment, and may inform risk management decisions. The techniques outlined in the Toolkit not only support the conduct of Business Process Analyses (BPAs) and Business Impact Analyses (BIAs) for continuity planning, but also may be applied to broader analytic endeavors.

The Toolkit is designed to increase risk awareness and enhance risk-informed decision-making processes within the federal, state, local, tribal, and territorial governments, and within critical infrastructure sectors. It serves as a continuity program resource that supports risk-informed analysis, and allows stakeholders to leverage its content to customize their respective analytic methods. The step-by-step instructions enable users to develop a systematic process for risk identification and mitigation, and to justify investment decisions to support continuity plans and programs.

Any comments or suggestions on the use of additional analytic techniques may be submitted to the Federal Emergency Management Agency (FEMA) National Continuity Programs at FEMA-NCP-Assistant-Administrator@fema.dhs.gov.



Roger L. Stone
Assistant Administrator (A)
National Continuity Programs

*The Continuity Risk Toolkit is a product of FEMA's National Continuity Programs,
based extensively on FEMA's The Full-Spectrum Risk Knowledgebase program, 2009-2014,
and developed with significant support from continuity and risk partners*

This page is intentionally blank.

INTRODUCTION

RISK 101

Ensuring a common understanding of risk – conceptually rather than through fixed terminology – is an important factor in analyzing and communicating risks and necessary for effective risk-informed decision making. While “risk” can be explained differently across disciplines depending on one’s focus and expertise or background, the concept remains the same. With a common understanding, subject-matter experts and stakeholders can speak through terminology and certain definitions to achieve the intended results of a risk study, or risk analysis.

Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.¹ With respect to continuity, analyzing risk through a Business Process Analysis (BPA) or Business Impact Analysis (BIA) aids in the validation of Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs) and in the identification of gaps in an organization’s operational processes and procedures, information technology (IT) and communication systems, and facilities. However, to ultimately inform leadership of what can happen (threats/hazards and outcomes), the likelihood of it happening (the combined probability of threats/hazards and vulnerabilities), and the consequences if it does happen (severity of outcomes), a more comprehensive approach to risk analysis is necessary.² Such risk analysis enables the systematic examination of the logical interaction of factors that contribute to threat, vulnerability, and consequence for the purpose of rank ordering scenarios according to their potential for causing harm or – for continuity programs – their potential for causing a degradation or hindrance in the performance of essential functions and supporting activities.

Risk analysis encapsulates information both on what may go wrong (risk assessment) and on what can be done to lessen the occurrence of certain threats/hazards or mitigate their consequences (risk management), as well as aid in characterizing uncertainties to enhance understanding of an organization’s risk profile. More specifically, a risk assessment is a product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.³ Risk management is the process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level, in consideration of associated costs and benefits of any action taken.⁴ Combined, these practices support comprehensive and effective analysis of all-hazards risk. Ultimately, among other benefits, all-hazards risk analysis will aid in the development of an effective continuity program and identifying, prioritizing, defending, and maintaining needed capabilities for a constant state of readiness.

¹ DHS Risk Lexicon. U.S. Department of Homeland Security, 2010.

² Kaplan, S. and Garrick, B. J. “On the Quantitative Definition of Risk.” *Risk Analysis*, Vol. 1, No. 1. 1981, pp. 11-27.

³ DHS Risk Lexicon. U.S. Department of Homeland Security, 2010.

⁴ DHS Risk Lexicon. U.S. Department of Homeland Security, 2010.

RISK ASSESSMENT

A risk assessment identifies and measures the threats (or hazards), vulnerabilities, and consequences facing an organization. In general, risk assessments seek answers to the following three questions:⁵

- What can happen?
- How likely is it to happen?
- What are the consequences if it does happen?

The results of a risk assessment – the answers to the above questions concerning the nature and magnitude of the assessed risks – are influenced by the knowledge of and information provided by subject-matter experts and key stakeholders, other available data, and the inherent randomness of certain events. More knowledge permits more focused decisions, whereas less knowledge requires more robust strategies. This requires risk assessments to balance reliance on the input of subject-matter experts and proven risk methodologies and tools to inform risk management strategies.

RISK MANAGEMENT

Risk management involves the consideration and implementation of strategies and measures to reduce the challenges identified in the risk assessment, and seeks to answer the following questions:

- What can be done?
- What are the trade-offs in terms of costs and benefits for each option?
- What impact will these options have on future efforts to mitigate risk?

Attention should also be given to questions concerning the tolerance for certain risks (i.e., are the risks acceptable or, rather, should something be done?) and the level of confidence in the analysis of data. While risk cannot be eliminated altogether, implementing mitigation options or countermeasures can aid in managing risks. These may take the form of policies and procedures, investments in equipment or technology, or improved training for personnel responsible for ensuring the continuation of essential functions. Ensuring redundant and diverse capabilities and the use of certain mitigation options or countermeasures may contribute to the deterrence of threats or the reduction of vulnerabilities, or lessen the extent of consequences resulting from the occurrence of a particular event or hazard identified through a risk assessment.

⁵ Kaplan, S. and Garrick, B. J. "On the Quantitative Definition of Risk." *Risk Analysis*, Vol. 1, No. 1. 1981, pp. 11-27.

LEVELS OF RISK ANALYSES

The development and organization of a specific analytic approach depends upon the level of analysis of the questions posed in a risk assessment. The approach outlined in this document allows for scalability and can be applied to multiple levels of an operation, organization, or region. This is especially key within continuity program management and planning, as the analysis will encompass multiple levels of an organization, internal and external stakeholders, and various threats and hazards. Examples of the scalability of an analysis are as follows:

- Strategic – Concerns the most significant questions of executive decision makers.
 - Regional or local threats that have a potentially devastating impact on operations.
 - Cost and benefit factors required for weighing different courses of action to reduce risk.
 - The extent and focus of risk management strategies – *How much* is enough and *where*?
- Operational – Concerns the decisions faced by operational-level decision makers.
 - For example, deployment of check points for screening versus high-profile patrols.
- Tactical – Concerns the likely risks of alternative tactical-level decisions.
 - For example, placements of vehicle barriers around a key facility.
- Programmatic (may apply at any of the above three levels)
 - Compares the risk reduction benefits of one or more programs.
 - Assesses the technological, cost, and/or schedule risks within a single program.

REPORTING ON RISK

A report summarizing the results of a risk analysis or assessment typically includes the following:

- Overview of key findings, summarizing analysis or assessment results;
- Description of scope, including the objectives of the assessment, questions to address for senior-level decision makers, and discussion of tolerance for loss or risk tolerance;
- Description of the organization or system, addressing the focus of the analysis and identifying interdependencies (internal and external) and criticality;
- Capabilities baseline, identifying and describing existing capabilities to manage or mitigate risk;
- Description of relevant threats and hazards and supporting information that informs likelihood of their occurrence;
- Description of the consequences of threats and hazards that provides context relevant to the organization and considering vulnerability (note that a vulnerability assessment must be conducted to inform consequence assessment);
- Results of the risk assessment, describing the organization's risk profile; and
- Risk management options that address improved capabilities or measures to mitigate risk and the potential for risk reduction.

In addition, the report should include supporting information that outlines the methodology and techniques used to perform the analysis, data sources, and subject-matter expert profiles or, at a minimum, the criteria used in subject-matter expert selection.

CONTINUITY PLANNING

Today's threat environment and the potential for no-notice events, including localized acts of nature, accidents, technological emergencies, and criminal or terrorist attacks, have increased the need for robust continuity capabilities and effective planning to enable organizations to continue to perform their essential functions across a broad spectrum of emergencies. Continuity planning is, simply put, a good business practice and, according to FCD 1, all Federal Executive Branch organizations, regardless of size or location, are required to have a viable continuity capability to ensure resiliency and continued performance of essential functions under all conditions.⁶ Risk analysis informs such planning and enables organizations to allocate resources to those areas of greatest risk and where the most benefit from investment may be achieved. Risk analysis, to include in the form of a BIA or BPA, will also aid in the identification of non-obvious risks and improvement not only to an organization's readiness for a continuity event but also strengthen its steady-state operations. As risk increases exponentially if capabilities are not available when needed, such as applications required for routine functions (distinct from those critical to the performance of essential functions), analysis will help an organization understand how it operates as a system and its interdependencies with other organizations. Understanding and addressing risk has innumerable benefits to mission execution and the performance of an organization's functions.

DESCRIPTION OF FUNCTIONS

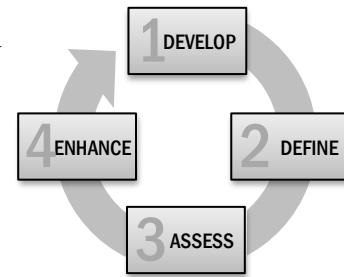
Organizations must incorporate continuity requirements into daily operations to ensure seamless continuation of essential functions and services. Therefore, the identification and prioritization of essential functions are a prerequisite for continuity planning to establish the parameters that drive an organization's efforts. Below is the list of functions defined in FCD 1.

- Government Functions:** All functions performed by an organization.
- Essential Functions:** Subset of Government Functions determined to be critical activities and that cannot be deferred during a disruption.
- Essential Supporting Activities (ESAs):** Activities required to support the performance of MEFs by 1) Protecting and Preserving Resources and/or 2) Reconstituting an organization's normal operations.
- MEFs:** Essential Functions directly related to accomplishing the mission of the organization.
- PMEFs:** MEFs validated by the National Continuity Coordinator that are required to support the performance of the NEFs before, during, and in the aftermath of a catastrophic emergency.
- NEFs:** NEFs are the functions of the Federal Government necessary to lead and sustain the Nation during a catastrophic emergency.

⁶ *Federal Continuity Directive 1*. U.S. Department of Homeland Security, Federal Emergency Management Agency, 2017.

CONCEPT OF OPERATIONS

The approach and techniques within the Continuity Risk Toolkit are designed to be used on a regular basis as part of a comprehensive continuity program that seeks to ensure risk-informed decision making. Each methodology and technique contained in the Toolkit can be associated with the following analytic themes or phases. Each phase is composed of multiple processes with corresponding information and materials to assist in conducting the analysis, and step-by-step guidance for each technique is included in appendices. The below Analysis Structure depicts the phases and processes used in risk analysis, and each phase is further described with examples of associated methodologies and techniques.



ANALYSIS STRUCTURE		
PHASES		PROCESSES
1	DEVELOP <i>the analysis by setting requirements and parameters.</i>	<input type="checkbox"/> Establish the justification and purpose for conducting the analysis. <input type="checkbox"/> Establish the analysis team, to include leadership and supporting staff. <input type="checkbox"/> Define the scope of the analysis. <input type="checkbox"/> Identify subject-matter expert criteria. <input type="checkbox"/> Review pre-analysis materials.
2	DEFINE <i>the focus of the analysis by conducting a business process analysis on the organization.</i>	<input type="checkbox"/> Identify the objectives of the organization. <input type="checkbox"/> Identify and describe the functions of the organization. <input type="checkbox"/> Map the functions to the objectives of the organization. <input type="checkbox"/> Conduct an essential functions analysis.
3	ASSESS <i>the potential risks to the organization through a risk assessment and analysis.</i>	<input type="checkbox"/> Conduct an all-hazards risk assessment. <input type="checkbox"/> Assess the vulnerability of each function. <input type="checkbox"/> Conduct a business impact analysis of all the functions. <input type="checkbox"/> Analyze and prioritize the identified risks.
4	ENHANCE <i>the readiness posture and preparedness of the organization by evaluating and recommending risk mitigation strategies.</i>	<input type="checkbox"/> Identify mitigation strategies. <input type="checkbox"/> Evaluate mitigation strategies. <input type="checkbox"/> Document the analytical process and results.

This page is intentionally blank.

ANALYSIS PHASES

PHASE 1: DEVELOP

The first phase in the analysis is to set requirements and parameters. This includes establishing the justification and purpose of the analysis and identifying the people (e.g., leadership, staff) who will be performing the analysis. This phase also requires defining the organization upon which the analysis will be performed and the scope of the analysis. This process is crucial as the framework for the analysis is designed to be flexible and cover a wide range of risk-based issues. When scoping for continuity, it is important to refer to federal guidance such as Federal Continuity Directives (FCDs). Another critical component of this first phase is the identification of subject-matter expert (SME) criteria. This step is vital as it will help to ensure quality input and adds credibility to the analysis and the defense of related recommendations.

Methodology/Technique	Reference	Section
Expert Opinion Elicitation Process (EOEP)	Appendix H	Step 2 through Step 5
Failure Modes and Effects Analysis (FMEA)	Appendix I	Part 1-1 through Part 1-5
Federal Continuity Directive (FCD) 1 Language	Not Applicable	Not Applicable
National Continuity Policy	Not Applicable	Not Applicable
System Description Methodology (SDM)	Appendix W	Step 1 and Step 2
Scoping a Risk Study	Appendix T	Step 1 and Step 2

1.1. ESTABLISH THE JUSTIFICATION AND PURPOSE

Before starting an analysis, the reasons for its conduct must be established and must include the types and nature of the decisions that it may or may not support considering the level of analysis. Most of the justification and purpose may already be developed depending upon the maturity of an organization's continuity program

and engagement with organization leadership. Language from FCD 1 further supports the justification and purpose of risk analysis as the Directive states that organizations must conduct risk assessments, to include Business Impact Analyses (BIAs), for all hazards and for all capabilities associated with the continuance of essential functions and such assessments will inform risk mitigation decisions. Other documents to draw justification and purpose from may include National Continuity Policy, organizational strategic plans, After-Action Reports from various exercises and real-world events, and improvement plans based on the Continuity Evaluation Tool (CET).

Methodology/Technique	Reference	Section
FMEA	Appendix I	Part 1-1
FCD 1 Language	Not Applicable	Not Applicable

This section may be completed using the steps and guidance provided in FMEA Part 1-1 using language from FCD 1 as justification and purpose.

1.2. ESTABLISH THE ANALYSIS TEAM

The justification and purpose of the analysis not only determines the level of the analysis but also the requirements for the analysis team. At a minimum, the team should be comprised of an individual that is familiar with the analysis process to serve as the team lead (e.g., Continuity Manager) and who has the ability to identify and reach out to people with the necessary expertise to inform the analysis. The analytic team lead will have the managerial and technical responsibility for the organization and execution of the risk analysis, participant oversight, and intellectual ownership of the results. The analytic team lead also has the responsibility of maintaining the professional integrity of the analysis and its implementation. Additional attributes of the team lead may include:

- Wide recognition and competence in performing risk analysis based on relevant experience, training, and certifications.
- Strong communication skills, interpersonal skills, flexibility, impartiality, and ability to generalize and simplify information.
- An ability to build consensus, and leadership qualities.

It is recommended the team lead rely upon the expertise of a team to support the analysis and that the team ensures quality assurance of the analysis processes and results through peer review. The ideal analysis team should consist of 5-7 individuals with complementary knowledge to support the analysis. For example, the team may consist of individuals with expertise in finance, information technology (IT), facilities, emergency management, security, business operations, and most importantly, all-hazards risk.

1.3. DEFINE THE SCOPE

A necessary element of a successful analysis is a clearly defined scope to establish the following:

- Boundaries for the analysis (what is and what is not considered).
- Definition or description of the organization and what about it is important in the context of the analysis.
- Threats and hazards that must be considered (accidental, random, deliberate, and malicious).

Methodology/Technique	Reference	Section
EOEP	Appendix H	Steps 2, 3
FMEA	Appendix I	Part 1-2

Both EOEP and FMEA complement each other and may be used in tandem or in lieu of each other; however, it is recommended to use EOEP as the primary source and FMEA as the secondary. The reason for this is due to EOEP being used as the primary source for SME elicitation throughout this document.

Methodology/Technique	Reference	Section
Scoping a Risk Study	Appendix T	Steps 1, 2
FMEA	Appendix I	Part 1-4
National Continuity Policy	Not Applicable	Not Applicable

"Scoping a Risk Study" is an extensive source of information; however, at this stage in the analysis, only Steps 1 and 2 should be utilized. FMEA is a secondary source for guidance and language from the National Continuity Policy can be used in conjunction to help define the scope.

In addition, logistics for the analysis (see FMEA Part 1-4) should be considered. Examples include 1) the nature of the analysis – whether it will be purely descriptive (i.e., qualitative) or have quantitative elements; 2) resources available for conducting analysis in terms of time, people, data, and timelines; and 3) constraints on the analysis, to include access limitations, information security requirements, etc.

The scope for the analysis is fairly well defined by language in National Continuity Policy and FCD 1. The analysis should consider all threats and hazards posed to an organization's essential functions and associated personnel and infrastructure. Continuity plans and procedures will be identified, assessed, and applied to ensure that appropriate operational readiness decisions are based on the probability of an attack or other incident and its consequences.

As the scope is defined, thought needs to be given to knowledge and the types of expertise needed to complete the analysis. This will assist in jump-starting the next step – building the criteria for identifying SMEs.

1.4. IDENTIFY SUBJECT-MATTER EXPERT CRITERIA

The analysis team must leverage additional SMEs, or panels of SMEs, for certain aspects of the analysis. Expert selection criteria is critical to establishing credible sources of information (i.e., SMEs). Individuals identified during the SME selection process should be familiar with the design, operation, and performance of the organization or with specific functions and should maintain a broad knowledge of the interdependencies across the organization. Although it is essential to select people with basic domain-specific, technological knowledge, it may be necessary to include one or two experts from management with technical knowledge of the organization's essential functions and supporting activities. Also, one or two experts with a background in all-hazards risk analysis and risk-based decision making may be needed. In order to identify a group of SMEs with the diversity and experience required for the success of the elicitation process, criteria such as the following should be defined.

- Strong relevant expertise.
- Familiarity and knowledge of various issues within the scope of the analysis.
- Willingness to act as a proponent or impartial evaluator.
- Availability and willingness to commit needed time and effort.
- Willingness to effectively prepare for discussions by performing independent research and/or through advance review of pertinent materials and to provide unbiased evaluations and interpretations of data and information.
- Strong communication skills, interpersonal skills, flexibility, impartiality, and ability to generalize and simplify information.

Methodology/Technique	Reference	Section
EOEP	Appendix H	Steps 4, 5
<i>EOEP Steps 4 and 5 go into the process of actually selecting experts. Some organizations may be capable of conducting this action at this stage of the analysis, but for many, the primary focus is developing criteria to be used further on to identify SMEs.</i>		
<i>EOEP Step 5 is optional; however, identified SMEs may want support staff to assist them in the analysis, and Step 5 touches on such support staff.</i>		

The size and number of expert panels will be determined on a case-by-case basis (e.g., number and size of Divisions and Offices and complexity of their functions). The size of an expert panel should be large enough to achieve diversity of opinions and credibility to produce reliable results, but small enough to ensure productivity and specific findings.

1.5. REVIEW PRE-ANALYSIS MATERIALS

The pre-analysis materials should clearly articulate the scope of the analysis, team composition, types of experts who will be consulted, any constraints on available resources, a concise definition or description of the organization, and, to the maximum extent possible, information on what is not to be covered in the analysis. Once complete, the analysis team lead must review the pre-analysis materials with the leadership (e.g., Continuity Coordinator) for concurrence before proceeding and to ensure clear understanding of the scope of the analysis and expectations of results.

Methodology/Technique	Reference	Section
FMEA	Appendix I	Part 1-5

Follow FMEA 1-5 to complete this section.

PHASE 2: DEFINE

The Define Phase of the analysis establishes an operational and architectural picture of the organization by breaking the organization down into interconnected functions with corresponding systems, personnel, and resources. This process is accomplished by performing a Business Process Analysis (BPA). Upon completion of the BPA, an essential function analysis may be conducted to determine and rank order the criticality of all the functions and categorize them by the definitions described in FCD 1 – government function, essential supporting activity (ESA), Mission Essential Function (MEF), and Primary Mission Essential Function (PMEF). The following methodologies and techniques are presented as options for completing an essential function analysis.

Methodology/Technique	Reference	Section
Anticipatory Failure Determination (AFD)	Appendix A	Steps 1, 2
Business Process Maps	Not Applicable	Not Applicable
Divergent-Convergent Thinking	Appendix C.3	All
Expert-Opinion Elicitation Process (EOEP)	Appendix H	Steps 6, 7, 8, 9
Essential Function Analysis	FCD 2	Not Applicable
Failure Modes and Effects Analysis (FMEA)	Appendix I	Part 2-1
SIPOC Diagram	Appendix U	All
System Description Methodology (SDM)	Appendix W	Steps 4, 5, 6, 7
Work Breakdown Structure (WBS)	Appendix Y	All

2.1. CONDUCT A BUSINESS PROCESS ANALYSIS

A BPA is a systematic method of identifying and documenting all organizational functions required to accomplish the objectives of the organization and the elements necessary to perform each function. It provides a method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, essential records, interdependencies, and facilities necessary for the execution of functions.

2.1.1. Identify the Objectives of the Organization

To “define” the organization, the objectives of the organization need to be identified. Objectives can normally be found in the organization’s mission statement, strategic plan or goals, or documentation on former PMEFs and MEFs.

Depending on the type of analysis being conducted (e.g., quantitative), the objectives may need to be rewritten to formulate them into terms of a specific level of performance. Example objectives are “generate greater than 10MW of electricity persistently” for a power plant or “maintain a 90% response time of 3 minutes and below for major emergencies” in the case of an emergency response unit. The purpose for defining objectives in terms of performance is to allow for a better understanding of capabilities when weighing and measuring risks. It also helps inform the next step – articulate a complete set of success scenarios.

A success scenario is a concise statement of how an organization must perform under all conditions by defining the boundary between failure and success. In regards to continuity, an organization may have at least two success scenarios describing the capability and duration of the organization under 1) normal operating conditions and 2) a catastrophic emergency, as defined in FCD 1. A baseline for a success scenario may be “continuously perform PMEFs

during continuity activation or resume MEFs within 12 hours of an event and sustain operations for a minimum of 30 days or until normal operations are resumed.” Consideration for other essential functions, facilities, communications, and staff must also be included in the success scenarios.

Methodology/Technique	Reference	Section
FMEA	Appendix I	Part 1-3
SDM	Appendix W	Steps 1, 2
AFD	Appendix A	Steps 1, 2
EOEP	Appendix H	Steps 6, 7, 8, 9

Use FMEA as a high-level guide for defining the organization with SMEs through use of EOEP. Follow up the FMEA with the SDM steps to further refine objectives and success scenarios and, if necessary, AFD for additional support.

2.1.2. Identify and Describe Organizational Functions

The first step in identifying an organization's functions is defining the internal and external variables – inputs, outputs, and state variables – using the EOEP methodology to garner expert opinions for each function. A top-down approach, such as the Work Breakdown Structure, will support the identification of functions as the analysis delves deeper into the organization.

Identification of outputs enables an assessment of how the function is performing, whereas inputs feed into the function to contribute to its performance. Inputs come in a variety of types, including decisions (inputs that are controllable by the decision maker), environmental (inputs from the environment, some of which might be random), and exogenous (inputs from outside the function). Depending on the function and its objectives, there may be multiple inputs.

State variables describe the properties of the function at any given time and are influenced by inputs and internal processes. State variables then directly influence the values of the outputs, and thus whether the function performs in accordance with the success scenario. For example, a state variable in an emergency response situation might be the number of available responders at a given time and number of active incidents. Combined, outputs and state variables influence the ability of the function to respond to an incident.

2.1.3. Map Functions to the Organization's Objectives

A process map provides a visual representation of the organization's functions and establishes a foundation for follow-on analysis. The map may have already been developed based on the procedures used in the previous step. Otherwise, the map can be developed using the SIPOC Diagram or Work Breakdown Structure, both of which could also be created during the initial identification of functions while collecting inputs, outputs, and dependencies.

It is recommended to consult with an organization's risk management staff and individual Divisions and Offices to develop or obtain process maps. From that point, or if no process maps exist, a recommended approach is to begin mapping at the function level and continue until the relationships between all the

Methodology/Technique	Reference	Section
WBS	Appendix Y	All
SDM	Appendix W	Steps 4, 5, 6, 7
SIPOC Diagram	Appendix U	All
EOEP	Appendix H	Steps 6, 7, 8, 9
Divergent-Convergent Thinking	Appendix C.3	All

Utilize the Work Breakdown Structure to segment the organization's objectives. As the objectives are divided, the SDM methodology may be used as a guide in identifying and refining organizational functions. SIPOC will assist in organizing the collected information. Information will be collected using EOEP – guidance in eliciting information from SMEs. The elicitation process can use a number of other methodologies, such as Divergent-Convergent Thinking (or other brainstorming techniques).

State variables describe the properties of the function at any given time and are influenced by inputs and internal processes. State variables then directly influence the values of the outputs, and thus whether the function performs in accordance with the success scenario. For example, a state variable in an emergency response situation might be the number of available responders at a given time and number of active incidents. Combined, outputs and state variables influence the ability of the function to respond to an incident.

Methodology/Technique	Reference	Section
SIPOC Diagram	Appendix U	All
Business Process Maps	Not Applicable	Not Applicable
WBS	Appendix Y	All

Based on the SIPOC Diagrams developed in the previous step, process maps may be developed to provide a visual representation of the workflow. This is an optional step as the SIPOC is more than capable of providing the information necessary to continue the analysis. The Work Breakdown Structure provides a simpler map.

functions are fully established and a visual representation of the support the functions provide to the objectives of the organization is visible.

2.2. CONDUCT AN ESSENTIAL FUNCTION ANALYSIS

The essential function analysis focuses on reviewing each function identified within the organization to determine which functions are potential MEF candidates. This process is described in detail in FCD 2 and focuses on determining if a function is mission essential, non-mission essential, or a supporting activity.

An activity that supports an organization's MEF is typically something unique to that organization; for example, providing assistance services to veterans is the responsibility of the U.S. Department of Veterans Affairs. On the other hand, a supporting activity is something most organizations do, such as providing IT support to the organization.

If the function results in the delivery of service to the public or another agency, it is likely essential to the mission of the organization (note: this is why it is important to identify outputs). If the function results in a service being delivered to another part of the same organization, it likely is a supporting activity. Supporting activities are typically enablers that make it possible for an organization to accomplish its mission, such as IT support provided by an Office of the Chief Information Officer or facilities management provided by the mission support or administrative component of an organization. The organization recognizes that it could not accomplish its missions efficiently without these supporting activities.

The distinction between these essential and non-essential functions is whether or not organizations must perform a function during a crisis. Essential functions are those that must continue during emergencies. Essential functions are both important and urgent. If an organization determines that a function would have to continue during or immediately after an emergency, that organization will identify it as essential. Functions that can be deferred until after the emergency will be identified as non-essential. Non-essential functions may be important, but are not as time-sensitive as essential functions.

PHASE 3: ASSESS

The pivotal point of the analysis is the Assess Phase; it is a holistic approach that hinges on a well-developed BPA. The Assess Phase uses risk assessment and analysis processes to identify potential failures, causes of the failures, and the impact from failure throughout all the functions in the organization. The all-hazards risk assessment will shift the focus of the analysis from the organization to external factors (i.e., threats and hazards). The EOEP methodology and SME criteria are critical to identifying the appropriate SMEs who can provide input on threats and hazards alongside information on vulnerabilities within the organization and its functions. Simply put, the goal of the analysis is to

Methodology/Technique	Reference	Section
FMEA	Appendix I	Part 2-1
Essential Function Analysis	FCD 2	Not Applicable

For the purpose of the analysis, FMEA Part 2-1 provides high-level guidance for identifying critical functions. The essential function analysis may also be conducted in conjunction with or following the FMEA to categorize each function in the respective continuity category.

determine all possible ways the organization can fail, and identify and prioritize risks to inform decisions aimed at lessening the likelihood of failure.

Methodology/Technique	Reference	Section
Expert-Opinion Elicitation Process (EOEP)	Appendix H	Steps 6, 7, 8, 9
Event Tree Analysis	Appendix G	All
Failure Tree Analysis (FTA)	Appendix J	All
Failure Modes and Effects Analysis (FMEA)	Appendix I	2-2, 3-1, 3-2, 4-1, 4-2, 6-1, 6-2, 6-4
Threat and Hazard Networks	Appendix Z	All, as applicable
Premortem Analysis	Appendix P	Steps 2, 3, 4, 5, 6
Root Cause Analysis	Appendix S	Steps 1, 2, 3, 4
Weighted Ranking	Appendix X	All

3.1. CONDUCT A RISK ASSESSMENT

The risk assessment's primary purpose is to identify how and why an organization can fail to meet objectives due to failure of its functions. It accomplishes this objective by examining all the previously identified functions to determine their failure modes, the likelihood of failure, and the severity of impact from failure.

3.1.1. Conduct an All-Hazards Risk Assessment

An all-hazards risk assessment will identify and correlate potential vulnerabilities and impacts from threats and hazards to an organization. The Threat and Hazard Networks serve as a resource to enable an in-depth analysis of various threats and hazards, which is critical to informing an organization's continuity program. Used with brainstorming techniques, the networks will help the analysis team and SMEs identify non-obvious risks, recognize additional interdependencies, and determine the extent of impacts from the consequences or cascading effects of an incident on the organization and the performance of its functions. Moreover, the use of a scenario is beneficial when working through questions as part of analysis; scenarios help frame questions for SMEs during elicitation sessions.

Overall, this step seeks to identify the reasons why failure of certain functions might occur by determining potential root causes. Depending on the scope of the analysis, causes might include accidental, technological, natural, and deliberate or malicious acts.

After root causes are identified, the analysis team will estimate the likelihood of occurrence for each root cause. This is referred to as the likelihood rating. Specifically, likelihood answers the following question:

Methodology/Technique	Reference	Section
FMEA	Appendix I	Parts 4-1, 4-2
Root Cause Analysis	Appendix S	Steps 1, 2, 3, 4
Threat and Hazard Networks	Appendix Z	All
EOEP	Appendix H	Steps 6, 7, 8, 9
FTA	Appendix J	All

Follow the FMEA and Root Cause Analysis techniques, along with associated brainstorming techniques and referencing Threat and Hazard Networks in conjunction with the EOEP methodology to assess risk. FTA may assist in providing a deeper dive into Root Cause Analysis and a more holistic picture of all threats and hazards.

How likely is it that the particular vulnerability will be exposed to the particular root cause? Scales for weighing and measuring likelihood may include quantitative scales (interval, ratio, and logarithmic scales) or non-numeric ordinal scales and scales based uncertainty measures.

It is important to maintain focus on the scope of the analysis when conducting a risk assessment, looking at risks that have a direct or indirect impact on operations of the organization and performance of essential functions.

3.1.2. Assess the Vulnerability of Each Function

During the risk assessment, it is important to identify all plausible ways failure could happen for each function – these are potential vulnerabilities. It may be helpful to focus on inputs, interdependencies, personnel, IT, and operational processes while applying one or more brainstorming techniques to answer the question of how the function can fail to meet its objective(s).

Methodology/Technique	Reference	Section
FMEA	Appendix I	Part 2-2
Premortem Analysis	Appendix P	Steps 2, 3, 4, 5, 6
EOEP	Appendix H	Steps 6, 7, 8, 9
Event Tree Analysis	Appendix G	All

FMEA may be used with Premortem Analysis in association with brainstorming techniques and the EOEP methodology. Event Tree Analysis may also assist in identifying vulnerabilities.

It is also helpful to use the success scenario – developed in the Define Phase – to provide context while conducting the all-hazards risk assessment, as well as heavily involving SMEs through the EOEP methodology. The results of past vulnerability assessments may further inform analysis, although certain areas may need to be revisited in consideration of the scope of the risk analysis being conducted.

3.1.3. Conduct a Business Impact Analysis (BIA)

The BIA estimates effects corresponding to the occurrence of failure of the function and identifies the consequences of exposure for each potential vulnerability (i.e., impacts), as well as the indirect impact or unintended consequences to external entities.

Methodology/Technique	Reference	Section
FMEA	Appendix I	Parts 3-1, 3-2
EOEP	Appendix H	Steps 6, 7, 8, 9
<i>Follow the FMEA in conjunction with the EOEP methodology.</i>		

Once the impacts are identified, the severity of each impact can be rated. Specifically, the analysis team and SMEs will answer the question of how severe the impact would be on the performance of the organization's objectives. Scales for weighing and measuring severity may include quantitative scales (interval, ratio, and logarithmic scales), non-numeric ordinal scales, or scales based on utility measures.

3.2. ANALYZE AND PRIORITIZE THE IDENTIFIED RISKS

The Analyze the Risks step will determine a rank order of risks and summarizes the entire analysis in the form of a risk register.

The rank order may be determined by the risk priority number, which results from the product of severity and likelihood rankings if using the FMEA

methodology. This number provides guidance for ranking potential failures in the order they should be addressed when identifying recommended mitigation strategies. This step, however, is not required to be done in this manner, and may be substituted with simple Sorting or Weighted Ranking, or augmented using quantitative risk analysis methods. The risk associated to *essential* functions must be identified and prioritized as well in order to enhance the identification and prioritization of risk mitigation strategies. Worksheets can aid in categorizing and sorting identified risks.

Methodology/Technique	Reference	Section
FMEA	Appendix I	Parts 6-1, 6-2, 6-3
Weighted Ranking	Appendix X	All
EOEP	Appendix H	Steps 6, 7, 8, 9

Follow the FMEA and associated brainstorming techniques in conjunction with the EOEP methodology. Weighted Ranking may be used in lieu of FMEA steps.

PHASE 4: ENHANCE

The purpose of the Enhance Phase is to evaluate the overall effectiveness of one or more potential risk mitigation options by considering the range of potential benefits and comparing alternatives to see which is best overall. This section references the Benefit-Cost Analysis (BCA) methodology, which provides a comprehensive list of factors and questions that are useful for comparing the merits of one or more potential mitigation options and enables evaluation of BCA results. However, it is up to the analysis team to determine the right questions for the decision at hand.

Methodology/Technique	Reference	Section
Benefit-Cost Analysis (BCA)	Appendix B.2	Benefit Assessment, Descriptive Elements
BCA	Appendix B.1	Steps 3, 4, 5
Expert-Opinion Elicitation Process (EOEP)	Appendix H	Steps 6, 7, 8, 9
Failure Modes and Effects Analysis (FMEA)	Appendix I	Part 6-3
Weighted Ranking	Appendix X	All

4.1. IDENTIFY MITIGATION STRATEGIES

The first step of the Enhance Phase is to identify one or more potential mitigation strategies, (also referred to as mitigation options, risk management options, or countermeasures) for reducing risk to an organization and performance of its functions by one or all of the following methods:

- Mitigating the likelihood of a threat/hazard
- Eliminating one or more vulnerabilities
- Reducing the severity of failure
- Improving resiliency, chiefly through redundancy and diversity

Before identifying a mitigation strategy as a recommended option to reduce risk, it is important to develop a detailed understanding of the option, including what it is, how it works (to include interdependencies), and how performance is measured. This is accomplished through the steps in BCA Descriptive Elements and by developing a full description of each potential mitigation strategy. A full description of the mitigation strategy requires knowledge of its functionality and reliable evidence (measured or estimated) of performance or non-performance of the mitigation strategy in the context of its intended usage.

4.2. EVALUATE MITIGATION STRATEGIES

The second step in identifying mitigation strategies is to compare alternatives on the basis of their potential benefits, detriments, and other factors.

The benefit of a mitigation strategy describes the value-add following its implementation and over its entire life cycle. The two benefits to account for when evaluating mitigation strategies are: 1) direct benefits – the extent to which the mitigation strategy reduces risk; and 2) secondary benefits – all benefits associated with a mitigation strategy other than direct benefits, to include impact on other risks, applicability to other problems, etc.

In addition to evaluating benefits, detriments (i.e., dangers of use) must also be evaluated. These include all new hazards or adverse impacts that can emerge from the use of a mitigation strategy. For example:

Methodology/Technique	Reference	Section
FMEA	Appendix I	Part 6-3
BCA	Appendix B.2	Descriptive Elements
EOEP	Appendix H	Steps 6, 7, 8, 9

Follow FMEA as the primary technique with BCA Descriptive Elements as a reference for questions to be asked for an in-depth approach to identifying mitigation strategies. EOEP will be used throughout the process to elicit input from SMEs.

Methodology/Technique	Reference	Section
BCA	Appendix B.2	Benefit Assessment
BCA	Appendix B.1	Steps 3, 4
Weighted Ranking	Appendix X	All
EOEP	Appendix H	Steps 6, 7, 8, 9

BCA Steps 3 and 4 will be used as the primary guidance with BCA Benefit Assessment as a reference for questions to be asked for an in-depth approach to evaluating mitigation strategies. Weighted Ranking may also support both techniques in measuring and visualizing the evaluations. EOEP will be used as necessary.

- Can the use of this mitigation strategy lead to unintended consequences such as hindering response capability or causing environmental damage?
- Can this mitigation strategy be exploited to cause harm?
- What other mitigation strategies do not work well with this option?
 - Under which circumstances do these detriments manifest?
 - Are these mitigation strategies present in the organization?

4.3. DOCUMENT ANALYTICAL PROCESS AND RESULTS

The final step involves documenting all of the methodologies and techniques used in the analysis and corresponding results as part of report development.

Methodology/Technique	Reference	Section
BCA	Appendix B.1	Step 5

Follow BCA Step 5.

- Compile all results and worksheets from the analysis
- Document the process and results in a report (see the Risk 101 section for typical report contents), appending all materials completed for each of the phases of the analysis
- Provide the report and all materials to key stakeholders and leadership (e.g., Continuity Coordinator) for review and validation

This page is intentionally blank.

METHODOLOGIES AND ANALYTIC TECHNIQUES

Appendix	Methodology/Technique	Description
A	Anticipator Failure Determination (AFD)	AFD is a problem-solving tool that is used to reveal potential failure modes in a system.
B	Benefit-Cost Analysis (BCA)	The purpose of a BCA is to evaluate the overall cost-effectiveness of one or more mitigation options – considering the range of potential benefits, costs, and other factors.
C	Brainstorming Techniques	Appendix covering a number of brainstorming techniques to support the implementation of the methodologies and analytic techniques described within the Toolkit
C	Delphi Method	The Delphi Method (also known as Delphi Technique) is a forecasting method that relies on obtaining a consensus from a collection of experts.
C	Devil's Advocacy	Devil's Advocacy involves challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation.
C	Divergent-Convergent Thinking	Divergent-Convergent Thinking is a form of structured brainstorming that generates new analytic ideas, hypotheses and concepts or helps discover previously unimagined hazards, vulnerabilities and risky situations through an unconstrained creative group process.
C	Outside-In Thinking	Outside-In Thinking is used to identify the full range of basic forces, factors, and trends that would indirectly shape an issue.
C	Round-Robin Brainstorming	Round-Robin Brainstorming relies on ideas being generated in the absence of discussion for completely free-form thoughts unhindered by group trends or consensus.
C	Reverse Brainstorming	Reverse Brainstorming is a structured brainstorming technique that asks how and why a hazard might not occur, and uses the converse of these reasons to suggest how it might actually occur.
D	Cause and Effect Diagrams	A Cause and Effect Diagram, also called a fishbone diagram or an Ishikawa Diagram, is a visual representation of possible contributing factors to an outcome of concern.
E	Developing Factor-Based Models	Factor-based models are a major part of Qualitative Risk Analysis, where the factors provide the means for breaking down complex problems into more manageable pieces.

Appendix	Methodology/Technique	Description
F	Event Mapping	Event Mapping organizes the who, what, where, when, why, and how of an event is the goal of this graphic organizer.
G	Event Tree Analysis	An Event Tree is a visual depiction of the downstream events resulting from the occurrence of an initiating event affecting a system.
H	Expert-Opinion Elicitation Process	Expert-opinion elicitation is defined as a formal, heuristic process of obtaining information or answers to specific questions about certain quantities, called issues, such as failure rates, probabilities of events, failure consequences and expected service lives.
I	Failure Modes and Effects Analysis (FMEA)	FMEA is a formal systematic approach to identifying how a system could fail, the causes of such failure, and the effects of its occurrence on the system operation.
J	Fault Tree Analysis (FTA)	FTA is a top-down approach for identifying how an undesirable event can happen or be made to happen. A Fault Tree systematically breaks down a single undesirable event in terms of its potential underlying causes.
K	Hazard and Operability Analysis (HazOp)	HazOp is a bottom-up approach that identifies potential hazards and operability complications within a system.
L	Hierarchical Holographic Modeling (HHM)	HHM is a technique for examining an issue from multiple points of view to identify the various sources of risk present in a large-scale system.
M	Influence Diagrams	An Influence Diagram (also known as a relevance diagram, decision diagram, or a decision network) is a compact visual representation of a decision situation that shows how a set of variables interact with one another.
N	Measurement of Intangibles	The ability to assign quantitative measurement to characteristics that are generally believed to be immeasurable.
O	Preliminary Hazard Analysis (PHA)	PHA is a semi-quantitative analysis that is implemented in the earliest stages of system design.
P	Premortem Analysis	Premortem Analysis allows a group of analysts or stakeholders (i.e., team) to examine the various factors that could inhibit the success of a plan.
Q	Problem Restatement and Issue Development	Problem Restatement and Issue Development is a technique used to ensure that the central issues and alternative explanations of an issue or problem are identified within the scope and focus of the problem statement
R	Reliability Block Diagrams (RBDs)	RBDs are graphical illustrations of how the failures of system components interact to cause failure of the entire system.

Appendix	Methodology/Technique	Description
S	Root Cause Analysis	Root Cause Analysis is a systematic approach that seeks to identify the origin of a problem.
T	Scoping a Risk Study	Scoping a Risk Study is a process of defining the scope and boundaries of a project utilizing multiple methodologies.
T	Scoping a Risk Study: Defining the Security Context	Defining the Security Context specifies the bounds on what is considered and what is not considered in a risk study.
T	Scoping a Risk Study: Defining a System	Defining a System is a concept that builds upon the security context by identifying what systematically decomposing a system into assets will directly bear on the interests of the protector.
U	SIPOC Diagram	SIPOC Diagram helps define the key elements, scope, and boundaries of a function.
V	Sorting	Sorting is a basic structured analytic technique for grouping information to develop insight, identify patterns, uncover trends, and spot anomalies.
W	System Description Methodology (SDM)	System Description Methodology provides an approach for completely describing a system of interest.
X	Weighted Ranking	Weighted Ranking is a technique for ranking and prioritizing different events, vulnerabilities, hazards, threats, countermeasures or other objects with respect to two or more value criteria.
X	Weighted Ranking: Pairwise Ranking	Pairwise Ranking is a technique for ranking a small list of items in priority order, whether by importance, preference or other measure of value.
Y	Work Breakdown Structure (WBS)	WBS is a dynamic process for defining the products of a project and their relationships.

This page is intentionally blank.

APPENDICES

APPENDIX A. ANTICIPATORY FAILURE DETERMINATION

What is it? Anticipatory Failure Determination (AFD) is a problem solving tool that is used to reveal potential failure modes in a system. In contrast to other analytic techniques for analyzing failure modes, AFD emphasizes Inventive Problem Solving combined with the Theory of Scenario Structuring.⁷ There are two variants to the AFD approach: AFD-1 (for failure analysis) and AFD-2 (for failure prediction).

- AFD-1 is used to find the cause of a system failure that has already taken place. This is also known as a post-mortem. This application of AFD supports Failure Analysis ([Appendix I](#)) or Root Cause Analysis ([Appendix S](#)).
- AFD-2 is used to understand how a system could fail at some time in the future and under different circumstances. This application of AFD supports Failure Prediction and complements Premortem Analysis ([Appendix P](#)) and a variety of other structured analytic techniques.

Why use it?

- **Provides common framework:**
 - AFD offers a common framework for both failure analysis (post-mortem analysis) and failure prediction (pre-mortem analysis). This feature may benefit institutions that train their employees in one methodology instead of several.
- **Provides a platform for creativity:**
 - AFD offers risk analysts the ability to append the typical “reactive” approach of risk analysis to a more pro-active one by allowing individuals to use existing data to invent new practical and realistic systems failures instead of trying to predict them to prevent the past events from reoccurring.
- **Focuses on problem solving:**
 - Previous analyses such as quantitative risk analyses ask basic questions such as, “What can go wrong?” whereas AFD-2 asks the question “If I wanted to make something go wrong, how could I do it in the most effective way?” This alternative approach promotes creative problem solving by risk analysts whereas the alternative approaches rely more heavily on what has happened in the past.

⁷ Kaplan, Stan, Yacob Y. Haimes, and B. John Garrick. “Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk.” *Risk Analysis*. Vol. 21, No. 5. 2001, pp. 807-820. <<http://onlinelibrary.wiley.com/doi/10.1111/0272-4332.215153/pdf>>.

Timing Define and Assess Phases for defining the organization/system and assessing the risks associated with the system. AFD can also be used to study the risk of system failure in all contexts, from business, technology and homeland security.

Some uses for the AFD methodology include:

- Reveal root causes of an error, unsuccessful action, manufacturing failure, or accident
- Predict future problems, accidents, errors, failures
- Develop effective and simple ways of preventing these problems
- View failure as a strategic objective and seek ways to deny success to those that attempt to cause failure

AFD complements a wide variety of other structured analytic techniques, including:

- Failure Modes and Effects Analysis ([Appendix I](#))
- Hazard and Operability Analysis ([Appendix K](#))
- Preliminary Hazard Analysis ([Appendix O](#))
- Risk Registers

Steps In an AFD-1, the process starts with a given end state or mid-state (i.e., the failure event has actually occurred) and a risk analyst must determine the actual scenario that led to the end or mid-state. An AFD-2 differs in that the process seeks to identify all possible end states, mid-states, and IEs as well as the scenarios that lead up to or occur after these states.⁸

The Anticipatory Failure Determination methodology is comprised of the following seven steps:

1. Formulate the “original problem”
2. Identify the success scenario
3. Localize the failure
4. Formulate and amplify the invert problem
5. Search for solutions
6. Formulate hypotheses and design tests to verify them
7. Correct the failure

⁸ Kaplan, Stan, Boris Zlotin, Alla Zusman, and Svetlana Visnepolschi. *New Tools for Failure and Risk Analysis: New Tools for Failure and Risk Analysis: Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring*. Southfield: Ideation International, 1999. Print.

A number of structured analytic techniques may help with performing different activities and steps associated with an AFD, including:

- Brainstorming Techniques, including Divergent-Convergent Thinking ([Appendix C.3](#)) and the Round-Robin Approach ([Appendix C.5](#))
- System Description Methodology ([Appendix W](#))
- Fault Tree Analysis ([Appendix J](#))

Cause and Effect Diagrams ([Appendix D](#))

Tips

Potential for infeasible scenarios: Encouraging analysts to create their own hypothesis on how an event happened could be a counter-productive process if not guided correctly. For example, less experienced analysts may divert attention towards completely infeasible ways a system could fail rather than focusing on the low-hanging fruit.

A.1. ANTICIPATORY FAILURE DETERMINATION STEPS

Step 1: Formulate the “original problem”

Create a detailed description of the system being analyzed. In order to complete this step, collect and document as much information about the goal of the failure event and both the aggregate and intricate system functions being analyzed. This process is referred to in this methodology as the “original problem” and used in AFD to describe system attributes, to include:

1. Naming the system
2. Stating the systems purpose
3. Describing the failure being analyzed

Step 2: Identify the success scenario

To further describe the system it is important to model its success scenario or the different phases of operation and the expected outcomes that must be met in each of the phases. A categorical way to dissect the system’s components are according to the following scheme:⁹

- Most critical
- Weak or dangerous functions
- Operations in the system

The outcome of this step will result in several models of failure scenarios that include both basic and intricate failure mechanisms.

Note: A way to graphically display the success scenarios of a system is by using a Reliability Block Diagram ([Appendix R](#)).

⁹ De Feo, Joseph A., and Zion Bar-El. “Creating Strategic Change More Efficiently with a New Design for Six Sigma Process.” *Journal of Change Management*. August 2002, pp. 60-80. <http://www.idealizationtriz.com/pdf_Creating_strategic_change.pdf>

Step 3: Localize the failure

Identify the phase or part of the system in which the actual event (or postulated event) has taken place. Through this process of localizing the failure, you are able to rule out parts of the system that could not cause a failure and thus reduce the area of analysis.

If you are completing an AFD-2 analysis, the failure has not occurred yet, but you will still be required to localize the hypothetical failure to a specific area of study.

Step 4: Formulate and amplify the invert problem

In Step 4, the goal is to restate the issue as a design problem and set the design objective such that failure would cause exaggerated consequences.

Part One (4-1): Invert problem. Creating an inverted problem requires restating the “original problem” identified in Step 1. This process of inversion forces analysts to change their approach from guessing the specific cause to developing various and creative ways to recreate the occurrence of the failure event.

- Example (Original Problem): How did Event Y occur?
- Example (Inverted Problem): How can I make Event Y can occur?

Original Question: How did this happen?



Inverted Question: How can I make this happen?

Use a pickaxe

to

Destroy a dam



Inverting a problem statement is a way for analysts to turn what was once a limited search for the specific cause of an event, into a broad and inventive approach that can result in several potential causes for a failure event.

Part Two (4-2): Amplify or exaggerate inverted problem. The contribution made by amplifying an inverted statement is that it makes the problem more vivid and further stimulates our inventive thinking.

Another important result of amplification is that the problem statement is now in a more useful form allowing an analyst to describe a problem so that its outcome is a method of production rather than simply, “How did this happen?” Now an analyst can provide solutions by asking, “How can I produce or create an event/failure?”

An example for incorporating amplification in an inverted problem is to consider a particular failure that takes place in a specific area, in some part of the surface or volume, or when a failure is rare or occurs from time to time. The amplified formulation would extend the inverted problem by appending the respective expressions:

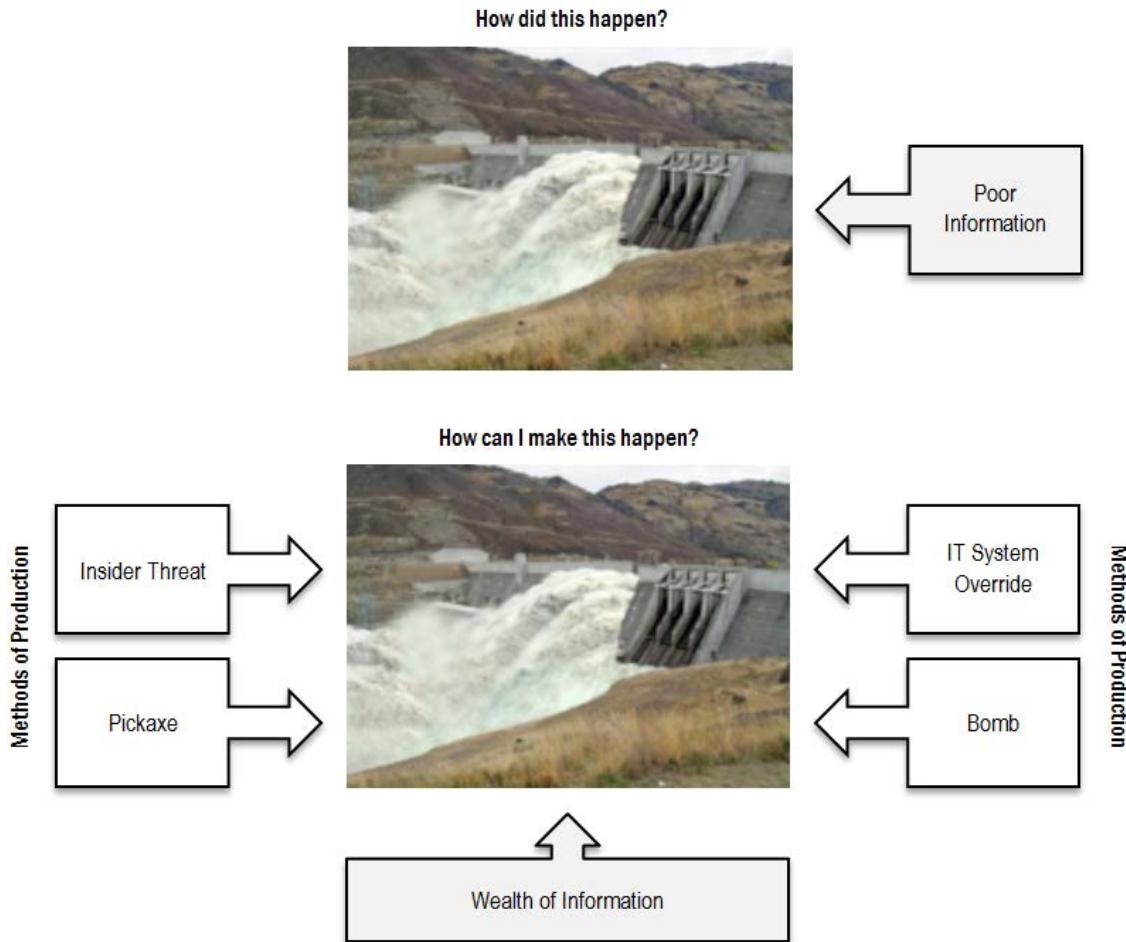
- “...over the entire surface”
- “...throughout the entire volume”
- “...”repeatedly” or “...constantly”

Step 5: Search for Solutions

In Step 5, the analysis has now shifted from the viewpoint of “things that can happen” to “things that can be produced.”

Part One (5-1): Search for apparent or obvious solutions. Once you have reached Step 5 you now have an inverted and amplified problem statement. Now you can begin to hypothesize methods for producing the failure event (e.g., pick axe or bomb destroying the wall of a dam). To start this examination, identify the areas of science, engineering, or even everyday life, where the same failure events have already occurred or have been intentionally created.

Once you begin to consider potential causes for failure that are apparent or obvious, you are able to move the analysis forward from a study, which had poor to no information, to a study which has a wealth of information. This added information increases the potential to further develop additional inventive methods and hypotheses.



Part Two (5-2): Identify Resources. To search for the necessary resources, one should do the following:

- Identify resources required for the occurrence of a given phenomenon/failure event
- Find necessary resources in the system or its surroundings

This step is used to take a systematic inventory of the resources available within the system or its environment (i.e., System Description Methodology [[Appendix W](#)]). Once the system's parts are specifically defined, the potential scenarios for failure will become clearer.

Part Three (5-3): Utilization of resources and searching for needing effects. If the required resources that have been identified in Part 5-2 are not commonly used or easily attained, it is necessary to create the resource or search for less obvious resources that can produce the failure phenomenon that will lead to the occurrence of the desired event.

Part Four (5-4): ARIZ (Algorithm for Inventing Problem Solving) for AFD. At this point in time, it is important to revisit the questions we have been asking in steps 5-1, 5-2, and 5-3, to include:

1. What physical effect or principle can create the desired failure?
2. What resources do I need to implement this principle?
3. What resources do I have?

In some cases the problem that exists may not be solved completely. Yet, there may be ways to solve for the cause of the desired failure in part. In these cases we develop a secondary problem.

1. Identify the “ideal solution”
2. The Innovation Guide
3. Targeting the technical and physical contradictions
4. Applying the separation principles
5. Substance-Field Analysis
6. The Operator Method

The utilization of ARIZ is the best way to invent the most complicated and non-trivial failures that can be associated with the system. A simplified version of ARIZ for AFD consists of the following steps:

1. Recap the problem
2. Formulate the secondary problem(s)
3. Formulate the ideal solution of the secondary problem
4. Search for ways to achieve the ideal solution

Step 6: Formulate hypotheses and design tests to verify them

Formulate the hypothesis as to how the failure occurred (or could occur) and specify whatever tests are required to prove this hypothesis (or demonstrate feasibility).

A hypothesis: is a proposed explanation for an observable phenomenon.

It is important that you formulate the hypothesis so that it can meet certain criteria so that others can replicate the same outcome.

Step 7: Correct the failure

If any failure hypothesis is seen as posing a significant risk to the system, this final step seeks to identify ways to prevent the failure from occurring again or ever occurring in the future.

The Failure Modes and Effects Analysis ([Appendix I](#)) is a methodology that identifies the various failure modes or vulnerabilities to a system. Applying this methodology could help to identify additional failures and suggested solutions.

This page is intentionally blank.

APPENDIX B. BENEFIT-COST ANALYSIS

What is it? The purpose of a Benefit-Cost Analysis is to evaluate the overall cost-effectiveness of one or more mitigation options – considering the range of potential benefits, costs and other factors. When more than one alternative is considered, Benefit-Cost Analysis is used to compare alternatives to see which is best overall.¹⁰

Why use it? Evaluation of countermeasures. The process seeks to evaluate, in words, the benefit to cost ratio of alternative countermeasures or mitigation options in a prescribed context.

Timing The identification of alternative countermeasures or mitigation options begins in the Enhance Phase. Components of the Benefit-Cost Analysis can be used in all phases of the risk analysis.

Steps The Benefit-Cost Analysis methodology is comprised of the following five steps:

Step 1: Characterize the System

- Define the objectives of the system as it relates to the decision maker
- Identify and describe the elements of the system
- Describe how these elements interact to achieve higher-level objectives

Step 2: Baseline Risk Assessment

- Understand how and why the system can fail to meet objectives due to failure of its basic elements
- Understand how and why the basic system elements can fail or be made to fail
- Understand the severity of each failure mode or scenario
- Understand the likeliness of occurrence for each failure mode or scenario

Step 3: Identify and Appraise Alternatives

- Develop a set of alternative countermeasures or mitigation options
- Develop a set of evaluation criteria consistent for each option considered
- Appraise each on the basis of the considerations described in the article on Benefit-Cost Analysis

¹⁰ This compiled methodology was developed in coordination with researchers at The Pennsylvania State University.

Step 4: Compare Alternatives

- Aggregate appraisals of evaluation into benefit and cost scores
- Compare the disaggregated scores
- Rank order alternatives

Step 5: Document the Analytic Process and Results**Tips**

In general, a countermeasure or mitigation option for which the benefits exceed the costs is considered to have merit as a viable alternative.

- For example, if we assess the benefit to be 3 and the costs to be 2 for a particular countermeasure or mitigation option, we would say this option has merit.
- If we assess the benefit to be 2 and the costs to be 3 overall, then we would argue against the merits of this option.

However, in some instances, particularly for security, it may be required that the benefit exceed the cost by a prescribed margin. In many instances, since security and risk mitigation investments do not produce a monetary gain, decision makers require that the benefit relative to cost exceed a margin.

- For example, if the required margin is 4, a countermeasure or mitigation option with a benefit of 3 and cost of 2 would not be considered to have merit as a viable alternative ($3 - 2 = 1 < 4$).

In general, it is very difficult to fully quantify in monetary terms all aspects of benefit and costs for any countermeasure or mitigation option.

B.1. BENEFIT-COST ANALYSIS STEPS

In this method, we define a meritorious countermeasure or mitigation option as one that:

- Has a favorable return on investment
- Is affordable
- Meets risk reduction objectives
- Satisfies all other constraints

Step 1: Characterize the System

If alternatives have not already been specified, this phase seeks to describe the system under study. The goals of this phase are:

- Define the objectives of the system as it relates to the decision maker
- Identify and describe the elements of the system
- Describe how these elements interact to achieve higher-level objectives

Methods to support this phase include (arranged from simple to complex):

- System Description Methodology ([Appendix W](#))
- Hierarchical Holographic Modeling ([Appendix L](#))
- Systems Dynamics Modeling

Note: This phase may be skipped if the system is thought to be well understood by the persons performing the Benefit-Cost Analysis. However, it is often helpful to perform the analysis in this phase anyway to ensure that this understanding is, in fact, not mired by invalid assumptions, stale preconceptions, etc.

Step 2: Baseline Risk Assessment

With a complete characterization of the system in hand, this second phase looks to examine how the system could fail, either due to accidental, random, deliberate, or malicious acts. The goals of this phase are:

- Understand how and why the system can fail to meet objectives due to failure of its basic elements
- Understand how and why the basic system elements can fail or be made to fail
- Understand the severity of each failure mode or scenario
- Understand the likeliness of occurrence for each failure mode or scenario

Methods to support this phase include:

- Failure Modes and Effects Analysis ([Appendix I](#))
- Divergent-Convergent Thinking ([Appendix C.3](#)) and other brainstorming techniques
- Event Tree Analysis ([Appendix G](#))
- Fault Tree Analysis ([Appendix J](#))

Step 3: Identify and Appraise Alternatives

This phase seeks to identify one or more candidate countermeasures or mitigation options for reducing all-hazards risk or that address a particular investment theme. The goals from this phase are:

- Develop a set of alternative countermeasures or mitigation options
- Develop a set of evaluation criteria consistent for each option considered
- Appraise each on the basis of the considerations described in the article on Benefit-Cost Analysis

Methods to support this phase include:

- Divergent-Convergent Thinking ([Appendix C.3](#))
- Weighted Ranking ([Appendix X](#))

Step 4: Compare Alternatives

This fourth phase seeks to compare alternatives on the basis of their potential benefits, costs and other factors. The goals of this phase are to:

- Aggregate appraisals of evaluation into benefit and cost scores
- Compare the disaggregated scores
- Rank order alternatives
- Challenge the results via alternative analysis

Methods to support this phase include:

- Weighted Ranking ([Appendix X](#))
- Sorting ([Appendix V](#))
- Devil's Advocacy ([Appendix C.2](#))

Step 5: Document the Analytic Process and Results

The final phase documents the analytic process and corresponding results. It is helpful here to append all worksheets completed for each of the methods used.

B.2. BENEFIT-COST ANALYSIS COMPONENTS

Benefit-Cost Analysis (BCA) estimates and totals up the value of all relevant benefits and costs associated with one or more investment options to establish whether they are worthwhile.¹¹ Benefit-Cost Analysis is also commonly known as Cost-Benefit Analysis (CBA). Some variants of BCA include Risk-Benefit Analysis and Cost-Benefit-Risk Analysis.

In general, a proposed countermeasure or mitigation option is considered viable if its overall benefit of use outweighs its cost of implementation. In some cases, the benefit must outweigh the cost by some appreciable margin. It is common to hear people speak of a variety of benefit-cost indicators for an investment option, including:

- NPV (net present value)
- PVB (present value of benefits)
- PVC (present value of costs)
- BCR (benefit cost ratio = PVB / PVC)

This section provides a comprehensive list of factors that are useful for appraising the merits of one or more candidate countermeasures or mitigation options in terms of benefits relative to costs.¹²

Accompanying each factor is a set of example questions a user might ask to better understand and assess the extent of benefit and magnitude of cost. However, it is up to the users to determine the right questions

¹¹ Watkins, Thayer. "An Introduction To Cost Benefit Analysis." San José State University. 2010.

<<http://www.sjsu.edu/faculty/watkins/cba.htm>>.

¹² This list of factors was developed by Dr. William McGill in coordination with researchers at The Pennsylvania State University. June 2009.

for the decision problem at hand. Each factor is noted as being applicable to one or more types of countermeasures or mitigation options, including:

- Asset (A)
- Human (H)
- Policy or Program (P)

To assist in performing a Benefit-Cost Analysis, refer to section B.1. Benefit-Cost Analysis Process Steps.

B.2.1. Descriptive Elements

Before performing a Benefit-Cost Analysis of any countermeasure or mitigation option, it is important to first understand its details, including what it is, how it works and how performance is measured. A full description of the countermeasure requires knowledge of its:

- Functionality
- Performance

Functionality

Functionality questions seek to describe what the countermeasure or mitigation option is and how it works or is supposed to work. (A/H/P)

Example questions include:

- What function does this countermeasure or mitigation option perform?
- What type of countermeasure or mitigation option is this (e.g., personnel, equipment, technology, tactics, techniques, procedures, planning, policy, training, etc.)?
- Does this countermeasure or mitigation option replace, upgrade, or augment a current countermeasure or mitigation option?
- Is this countermeasure intended to increase redundancy or diversity?

(Note: A *redundant* capability will include multiple systems to maintain functionality in case of the failure of the primary system. A *diverse* capability will include geographically or physically disperse systems that do not rely on common infrastructure to function, thus limiting back-up system exposure to the same threats/hazards as the primary system. A *redundant and diverse* capability will help ensure resilience, such as an information technology system that includes multiple servers located in different parts of the country and that rely on different network and supporting infrastructure to function.)

- In what innovative (non-conventional) ways has this countermeasure been applied?

Performance Measures

Performance measures provide reliable measurable evidence of performance or non-performance of the countermeasure or mitigation option in its usage context. (A/H/P)

Example questions include:

- How is the performance of this countermeasure or mitigation option specified and measured?
- What are the operational limitations of performance?
- In what environments has this countermeasure or mitigation option been used and performed as intended?
- In what environments has this countermeasure or mitigation option been used and failed to perform as intended?
- In what environments has this countermeasure or mitigation option not been used?
- How is this countermeasure or mitigation option tested and evaluated?
- Are there testing standards for this countermeasure or mitigation option?
- How do similar alternatives compare?
- How can we measure any change in overall system performance following implementation of the countermeasure or mitigation option?

B.2.2. Benefit Assessment

The benefit of a countermeasure or mitigation option describes the value-added, independent of cost, following its implementation over its entire life-cycle. The factors that shape an overall assessment of lifecycle benefit include:

- Viable Life
- Direct Benefits
- Secondary (Collateral) Benefits
- Dangers of Use
- Performance Deterioration
- Synergies
- Detriments

Viable Life

Viable life considers the duration in which the countermeasure or mitigation option will continue to operate as designed. (A/P)

Example questions include:

- What is the expected lifetime of this countermeasure or mitigation option?
- Does the lifetime of this countermeasure or mitigation option match, exceed or fall-short of the planning horizon?
- Can this countermeasure or mitigation option be readily uninstalled or abandoned if it fails to perform?

Direct Benefits

Direct benefits describe the extent to which the countermeasure or mitigation option reduces risk. (A/H/P)

Example questions include:

- What hazards and threats does this countermeasure or mitigation option work against?
- How does the countermeasure or mitigation option work to mitigate risk?
- What causal relationships between hazards does it mitigate, and to what extent? (see network linkages, [Appendix Z](#))
- What is the rate of occurrence of those linkages?
- What is the severity of those occurrences?
- Does the countermeasure or mitigation option provide any dissuasive value?
- What hazards are associated with employing this countermeasure or mitigation option?
- What attacker opportunities are created by this countermeasure or mitigation option?
- Is your organization, jurisdiction, or region already covered by the employable range of a neighboring entity's countermeasure or mitigation option?
- Will this countermeasure help build existing capability or prevent failure of related measures?

Secondary (Collateral) Benefits

Secondary (or collateral) benefits include all benefits associated with a countermeasure or mitigation option other than direct benefits, to include impact on other risks, applicability to other problem domains, etc. (A/H/P)

Example questions include:

- What other purposes can this countermeasure or mitigation option perform outside of its decided purpose?
- How does the countermeasure or mitigation option influence, for good or ill, the performance of other countermeasure or mitigation options in the field?
- Does the countermeasure or mitigation option perform any mundane function outside of its hazard-mitigation role, and what is the value of that role?
- Is the employable range of this countermeasure or mitigation option large enough to encompass other organizations, jurisdictions, or regions?

Dangers of Use

Dangers of use include all new hazards that emerge from the use of a countermeasure and mitigation option. (A/H)

Example questions include:

- Can the use of this countermeasure or mitigation option lead to unintended consequences such as hindering response capability or causing environmental damage?
- Can this countermeasure or mitigation option be exploited to cause harm?

Performance Deterioration

Performance deterioration of a countermeasure or mitigation option considers the degradation in countermeasure performance with time due to natural, attacker and defender-related causes. (A/H)

Example questions include:

- How does performance of this countermeasure or mitigation option degrade with time, and is the cause of this degradation from environmental wear, poor maintenance, or poor construction?
- Are there simple ways an adversary can circumvent this countermeasure or mitigation option?

Synergies

Synergies are the added benefits that occur due to the favorable interaction of this countermeasure or mitigation option with other countermeasures or mitigation options. (A/H/P)

Example questions include:

- Does the performance or lifespan of this countermeasure or mitigation option increase when used with other countermeasures or mitigation options?
- If so, which show the greatest gains and under which circumstances do these gains manifest?
- Are these countermeasures or mitigation options present in the system?

Detriments

Detriments are the decrease in benefits due to the unfavorable or conflicting interaction of this countermeasure or mitigation option with other countermeasures or mitigation options. (A/H/P)

Example questions include:

- What other countermeasures or mitigation options do not work well with this countermeasure or mitigation option?
- If so, under which circumstances do these detriments manifest?
- Are these countermeasures or mitigation options present in the system?

B.2.3. Cost Assessment

The costs of a countermeasure or mitigation option describe the value of resources required to acquire, implement, sustain, and phase out the investment over its entire life cycle. The factors that shape an overall assessment of life-cycle costs are:

- Acquisition Costs
- Operational & Maintenance Costs
- Supporting Infrastructure
- Training
- Salvage and Disposal
- Peripheral Costs

Acquisition Costs

Acquisition costs are the costs to acquire the countermeasure or mitigation option, to include the costs of purchase, installation, shipping and delivery, applicable taxes, etc. (A/H)

Example questions include:

- What is the range of costs for this countermeasure or mitigation option and what factors drive this range?
- How much does the countermeasure or mitigation option cost to buy?
- Are there installation or ramp-up costs?
- How much does the countermeasure or mitigation option cost to deploy?
- What factors drive acquisition cost for this countermeasure or mitigation option?
- Is the countermeasure or mitigation option commercial-off-the-shelf, readily trainable, borrowed from other organizations, jurisdictions, etc.?
- Is the countermeasure or mitigation option novel?
- Is this countermeasure or mitigation option expected to be less expensive in the future? If so, when?

Operational and Maintenance Costs

Operational and maintenance (O&M) costs include the costs to operate the countermeasure or mitigation over the course of its lifecycle, maintenance, repair, upgrades, etc. (A/H)

Example questions include:

- What factors drive operational cost for this countermeasure or mitigation option?
- How much does the countermeasure or mitigation option cost to run? To keep running?
- What costs are recurring in terms of consumables, resources, manpower, etc?
- Are they persistent, increasing with time, decreasing, dependent on use, or vulnerable to supply availability?

- What factors drive maintenance cost for this countermeasure or mitigation option?
- How long will it take for this countermeasure or mitigation option to become obsolete relative to a newer version?
- Can parts required for this countermeasure or mitigation option to operate be stockpiled?

Supporting Infrastructure

Supporting architecture costs include costs of parts, tools, policies, personnel, etc. outside of the basic countermeasure or mitigation option system. (A/H/P)

Example questions include:

- What other capabilities, tools, processes, training, organizational structures, installations, etc. are necessary for this countermeasure or mitigation option to function at full performance?

Training

Training costs are the costs to train personnel on the proper use and implementation of a countermeasure or mitigation option. This includes training on how to operate a device, training on how to adhere to a policy and training on how to perform a specific activity. (A/H/P)

Example questions include:

- Who needs to be trained in the use or deployment of this countermeasure or mitigation option?
- What factors drive training cost for this countermeasure or mitigation option?

Salvage and Disposal

Salvage and disposal costs are the costs associated with the end of a countermeasure or mitigation option's life, to include the costs of disposal minus the return for its salvage value. (A)

Example questions include:

- What are the costs to retire and dispose of this countermeasure or mitigation option?
- Is replacement included in the cost estimate?
- Does this countermeasure or mitigation option have a salvage value?

Peripheral Costs

Peripheral costs are the potential future costs due to regulation, litigation, and so on that might occur due to the use and implementation of a countermeasure or mitigation option. (A/H/P)

Example questions include:

- Has this countermeasure or mitigation option been the subject of public lawsuits due to pollution, invasion of privacy, safety, improper use, or other legal entanglements?
- Could use of this countermeasure or mitigation option result in liabilities for similar events?
- Does the countermeasure or mitigation option result in any negative externalities in the community?

B.2.4. Other Considerations

Beyond benefit and cost considerations, decision makers must also consider a variety of other non-enumerable factors that shape the appropriateness of a proposed countermeasure or mitigation option. Such factors include:

- Feasibility of Implementation
- Time to Full Performance
- Performance Monitoring
- Constituent Response
- Impact on Future Options

Feasibility of Implementation

Feasibility of implementation considers whether the countermeasure or mitigation option can be feasibly put in place in the intended situation or context. (A/H/P)

Example questions include:

- What are the constraints for the implementation of this countermeasure or mitigation option? (physical, social, fiscal, political, legal, and resource limiters)

Time to Full Performance

Time to full performance is the time it takes for the countermeasure or mitigation option to perform at the intended levels. (A/H/P)

Example questions include:

- How long does it take to ramp up to full performance from selection to implementation of the countermeasure or mitigation option?
- What factors delay or speed this process?
- What are the intermediary steps in this process for this countermeasure or mitigation option?
- Is the countermeasure or mitigation option currently ready for deployment? If not, when is the expected readiness date?

Performance Monitoring

Performance monitoring considers the extent to which the performance of the countermeasure or mitigation option can be monitored, assessed and evaluated. (A/H/P)

Example questions include:

- What are the constraints for monitoring the performance of this countermeasure or mitigation option?
- How is it suggested that performance is assured throughout the life of this countermeasure or mitigation option?

Constituent Response

Constituent response considers how people will respond to the installation and use of the countermeasure or mitigation option. (A/H/P)

Example questions include:

- How will employees react to the installation of this countermeasure or mitigation option? Will information on use of this countermeasure or mitigation option be widely messaged to employees, and how? Is union notification required?
- Is use of this countermeasure or mitigation option allowed under lease agreements, etc.? Is coordination with property managers required?
- How will the public react to the installation of this countermeasure or mitigation option? Is coordination with local officials appropriate?

Impact on Future Options

Impact on future options considers what future options, in general, are enabled or removed after the installation of a countermeasure or mitigation option. (A/H/P)

Example questions include:

- How does this countermeasure or mitigation option impact future decisions on investments in countermeasure or mitigation options or risk mitigation strategies?

This page is intentionally blank.

APPENDIX C. BRAINSTORMING TECHNIQUES

Page	Brainstorming Technique	Description
C-2	Appendix C.1 Delphi Method	The Delphi Method (also known as Delphi Technique) is a forecasting method that relies on obtaining a consensus from a collection of experts.
C-8	Appendix C.2 Devil's Advocacy	Devil's Advocacy involves challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation.
C-10	Appendix C.3 Divergent-Convergent Thinking	
C-19	Appendix C.3.a CIA Approach to Divergent-Convergent Thinking	Divergent-Convergent Thinking is a form of structured brainstorming that generates new analytic ideas, hypotheses and concepts or helps discover previously unimagined hazards, vulnerabilities and risky situations through an unconstrained creative group process.
C-22	Appendix C.3.b DIA Approach to Divergent-Convergent Thinking	
C-25	Appendix C.4 Outside-In Thinking	Outside-in thinking is used to identify the full range of basic forces, factors, and trends that would indirectly shape an issue.
C-26	Appendix C.5 Round-Robin Brainstorming	Round-Robin Brainstorming relies on ideas being generated in the absence of discussion for completely free-form thoughts unhindered by group trends or consensus.
C-28	Appendix C.6 Reverse Brainstorming	Reverse Brainstorming is a structured brainstorming technique that asks how and why a hazard might not occur, and uses the converse of these reasons to suggest how it might actually occur.

This page is intentionally blank.

C.1. DELPHI METHOD

What is it? The Delphi Method or Delphi Technique is a forecasting method that relies on obtaining a consensus from a collection of experts. This technique eliminates committee activity among the experts altogether and replaces it with a carefully designed program of sequential individual interrogations, usually in the form of a questionnaire.¹³ This consensus is reached through the idea that when given a summary of the group's first round of forecasts, experts will adjust their original answer to closer match that of their peers. After several rounds of adjustments the group converges on an agreed upon forecast or range of forecasts.

Why use it? This method provides decision makers with the ability to gain insight into future events through the consensus of experts in a respective field. Through the constraints of the process, decision makers can be assured of the outcome of these panels.

The Delphi Method offers two important characteristics in a group elicitation session:

1. Anonymity among group members: used to encourage diverse opinions
2. Controlled feedback: responses from the group are gathered and fed back to the group

Unlike other brainstorming techniques, the Delphi Method can be conducted asynchronously.

Timing This technique is designed to be used when decision-making is based on forecasting future events. A common use is the interpretation of economic models, which are subject to intuitive intervention. Similarly, in forecasting extreme events such as the weather or natural disasters, there is a need to rely on intuitive expertise as well. The Delphi Method has been used in many forecasting environments and may be often used in a government setting when performing cost-benefit analyses.

¹³ Helmer, Olaf. *Analysis of the Future: The Delphi Method*. Santa Monica: Rand, 1967. Print.

Steps	The overall approach for this methodology typically follows a four step, 10-part procedure: ¹⁴
	<ol style="list-style-type: none">1. Delphi technique planning and organization<ol style="list-style-type: none">a. Formation of a Delphi Monitoring Team to undertake and monitor a Delphi activity on a given subject.b. Selection of one or more panels to participate in the exercise.2. First round of Delphi questionnaire<ol style="list-style-type: none">a. Development of the first round of Delphi questionnaire.b. Testing questionnaire for proper wording (e.g., ambiguities).c. Transmission of the first questionnaire to the panelists.d. Analysis of the first round of responses.3. Second round of Delphi questionnaire<ol style="list-style-type: none">a. Preparation of the second round questionnaire (and possible testing).b. Transmission of the second round questionnaire to the panelists.c. Analysis of the second round of responses (Steps 3-a to 3-c are reiterated as long as desired or necessary to achieve stability in results).4. Prepare a summary report

Tips	The Delphi Method's overall track record is mixed. In dealing with forecasting there is a great deal of uncertainty which results in the ability to consistently produce accurate prediction as nearly impossible. If a group of panelists are misinformed about a topic it may produce inaccurate forecasts, which is only further supported by the other members of the group.
-------------	--

C.1.1. Delphi Method Steps

Step 1: Delphi technique planning and organization

- a. **Formation of a Delphi Monitoring Team to undertake and monitor a Delphi activity on a given subject.** Members of a Delphi team include a moderator (face of the process) and support staff responsible for interpreting the question, selecting the experts, developing and disseminating the Delphi questionnaire, and collecting and compiling the results.
- b. **Selection of one or more panels to participate in the exercise.** Customarily, the panelists are experts in the area to be investigated. The participants are the “subject-matter experts” chosen

¹⁴ Fowles, Dr. Jib, and Robert B. Fowles. *Handbook of Futures Research*. Westport: Greenwood, 1978. Print.

because of their unique expertise in one or more subject areas. To gain a well-rounded response, it has been suggested that the group of experts come from diverse backgrounds.

Step 2: First round of Delphi questionnaire

- a. **Development of the first round of Delphi questionnaire.** Typically the questionnaire consists of about 10 items where each expert is asked to rank or make some judgment about each.
- b. **Testing questionnaire for proper wording (e.g., ambiguities).** This step is performed by the Delphi Monitoring Team. The goal is to refine the wording of the questionnaire to minimize the chances of or prevent any confusion or misinterpretations by the experts. This can be done by conducting several or more trial surveys with experts from outside the monitoring team of participant pool.
- c. **Transmission of the first questionnaire to the panelists.** This can be done electronically via email or a website or through the postal service. This transmission should include any and all (objective) background data that might be helpful for the expert to understand the problem and render credible judgments.
- d. **Analysis of the first round of responses.** This analysis step focuses on where the participants agree and disagree as a group.

Step 3: Second round of Delphi questionnaire

- a. **Preparation of the second round questionnaire (and possible testing).** In general, the questionnaire does not change between rounds. The second round is meant to provide the participants with an opportunity to revise their opinions and judgments based on the summary of the group results and basis for their conclusions.
- b. **Transmission of the second round questionnaire to the panelists.**
- c. **Analysis of the second round of responses (Steps 3-1 to 3-3 are reiterated as long as desired or necessary to achieve stability in results).** The Delphi Moderator Team here is looking to see whether the group arrived at a consensus.

Depending on the size of the panel selected to provide input to the Delphi process, it may take more than two rounds to acquire a consensus. If this is the case, repeat all of Step 3 until either consensus is achieved or the resulting insight is sufficient to inform the end-user of the results.

Step 4: Prepare a summary report

Preparation by the Delphi team of a report at the conclusion of the exercise that describes its outcomes.

C.1.2. Illustrative Example

The following example describes a study supporting the work of the National Maritime Security Advisory Committee (NMSAC), which is charged by the Secretary of Homeland Security to advise the U.S. Coast Guard (USCG) on matters of maritime security. The particular key risk question of interest was as follows: *Rank order on the basis of relative likeliness a set of at least ten risk events that can affect maritime security in the next year.*

Step 1: Delphi technique planning and organization

Part One (1-1): Formation of a team to undertake and monitor a Delphi activity on a given subject

The research team was formed to offer a diverse group of members to monitor this project. Members included:

- Engineering professor (member of NMSAC)
- USCG advisor (Congressional mandate)
- Master's thesis student

Part Two (1-2): Selection of one or more panels to participate in the exercise. The panelists for this project were selected for their expertise in maritime security.

By law, the USCG controls shipping in the United States ports and therefore is knowledgeable of all sectors of the maritime domain. A USCG consultant assisted in the selection process of the following specialists:

- Public port expert
- USCG expert (port operations)
- Shipping expert
- Private ports/docks representative
- Law enforcement official

Step 2: First round of Delphi questionnaire

Part One (2-1) / Part Two (2-2) / Part Three (2-3): The questionnaire shown below was prepared for the specialists (and subject to testing for ambiguities). Accompanying the questionnaire was some historical data on past events such as hurricanes and other natural disasters and detailed instructions on ranking events (e.g., Pairwise Ranking).

Sr. No.	List of “Events”	Likelihood Scale 1 (Most Likely) to 10 (Least Likely)
1	Major vessel accident causing waterway closure or disruption of vessel traffic for more than one hour. (Unintentional, Human Error)	
2	Major oil spill/leakage affecting the Sabine - Neches Waterway (Unintentional)	
3	Port facility infrastructure breakdown (Unintentional)	
4	Damage to port facility, from a vessel equipment failure/malfunction (Unintentional, Navigational)	
5	Terror threat (hoax) - causing shutdown of port facilities or parts of the Sabine - Neches Waterway	
6	Damage or destroy a large vessel or tanker with the help of a small vessel approaching it with an explosive on board. (Terrorist Acts, USS Cole-Type Acts)	
7	Disruption of port facilities and/or operations by destroying key assets or	

Sr. No.	List of “Events”	Likelihood Scale 1 (Most Likely) to 10 (Least Likely)
	infrastructure such as cranes, electrical power systems, etc. (International, Terrorist Acts)	
8	Introduction into the United States of a weapon of mass destruction via the Sabine - Neches Waterway. (Intentional, Terrorist Acts)	
9	Coastal storms and hurricanes up to category II (Natural Disaster)	
10	Category III, IV, or V hurricanes (Natural Disaster)	
	Suggest Additional “Events” if you choose	
A		
B		

Part Four (2-4): The following results were collected from the first round.

Panel Members	Group 1		Group 2		Group 3		Group 4		Group 5		Survey Round 1 (SR1) Analysis			
	Public Ports		USCG		Shipping Industry		Private Ports		Law Enforcement		Quantitative tabulation of responses from participants			
Responses for the Rankings	SP1	SP2	SP1	SP2	SP1	SP2	SP1	SP2	SP1	SP2	Avg.	Low	High	Rank
Event 1		1	2	1	1	1	1	1	2		1.2	2	1	1
Event 2		5	1	2	2	4	2	2	1		2.3	5	1	2
Event 3		6	8	3	6	6	6	4	5		5.5	8	3	6
Event 4		4	5	4	7	5	3	3	4		4.3	7	3	4
Event 5		7	9	5	5	7	5	6	6		6.2	9	5	7
Event 6		8	6	9	9	9	9	7	9		8.2	9	6	9
Event 7		9	7	8	8	8	7	9	8		8.0	9	7	8
Event 8		10	10	10	10	10	10	10	10		10.0	10	10	10
Event 9		2	3	6	3	3	4	5	3		3.3	6	2	3
Event 10		3	4	7	4	3	8	8	7		5.5	8	3	5

Step 3: Second round of Delphi questionnaire

Part One (3-1) / Part Two (3-2): The second round questionnaire was prepared (same questionnaire as before) and was transmitted to the participants along with complied data form the previous survey round. The data added to the survey include Average Value, Low Value, High Value, Round 1 Priority Ranking.

Part Three (3-3): An analysis was conducted of the second round results as shown in the following table.

Panel Members	Group 1		Group 2		Group 3		Group 4		Group 5		Survey Round 2 (SR2) Analysis			
	Public Ports		USCG		Shipping Industry		Private Ports		Law Enforcement		Quantitative tabulation of responses from participants			
Responses for the Rankings	SP1	SP2	SP1	SP2	SP1	SP2	SP1	SP2	SP1	SP2	Avg.	Low	High	Rank
Event 1	1	3	2	2	1	1	1	2			1.6	3	1	1
Event 2	5	2	3	3	4	2	2	1			2.7	5	1	3
Event 3	6	7	4	5	5	6	5	5			5.3	7	4	5
Event 4	4	4	5	4	3	3	3	4			3.7	7	3	4
Event 5	7	9	6	6	7	5	6	6			6.5	9	5	7
Event 6	8	6	9	8	9	9	8	9			8.2	9	6	8
Event 7	9	8	8	9	8	7	9	8			8.2	9	7	9
Event 8	10	10	10	10	10	10	10	10			10.0	10	10	10
Event 9	2	1	1	1	2	4	4	3			2.2	4	1	2
Event 10	3	5	7	7	6	8	7	7			6.2	8	3	6

Step 4: Preparation of a report

A report was prepared describing the names of the participants, survey instrument (questionnaire) and results from all rounds. A summary of the results from this exercise is shown in the table below.

Survey Results		
Events	Round 1 Rank	Round 2 Rank
Event 1(major vessel accident, E1)	1	1
Event 2 (major oil spill, E2)	2	3
Event 3 (facility damage due to navigational error)	6	5
Event 4 (facility damage due to equipment failure)	4	4
Event 5 (terror threat-hoax)	7	7
Event 6 (USS Cole-type terrorist act)	9	8
Event 7 (facility damage due to terrorism)	8	9
Event 8 (intro. of weapons of mass destruction)	10	10
Event 9 (coastal storms)	3	2
Event 10 (category III or above hurricane)	5	6

C.2. DEVIL'S ADVOCACY

What is it? Devil's Advocacy involves challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation.¹⁵ This method has a group coming together to contradict the current position or belief of the group. The goal of the technique is to stretch the scope of what the group is considering.

Why use it? Generates alternate explanations. Devil's Advocacy is a great way to generate a set of possible explanations. Also, similarities across these explanations can help identify problem areas to be fixed. This methodology will assist analysts in identifying the best possible solution to a problem.

Timing Analysts and individuals have a tendency to come up with an idea, declare it the most suited for the problem at hand, and not consider alternative solutions. This methodology will attempt to break the individual or group from those beliefs and reassess all the possible ideas for which are best.

Steps The overall approach for this methodology is comprised of three steps:

1. Identify and research a position that is completely contrary to the current best position
 2. Confront the group or individual with the new position
 3. Reassess all of the possible solutions to choose the best one
-

Tips **Requires subject-matter experts.** As with many methodologies, this one depends entirely on the analyst to properly generate the alternative explanation. Involving as many subject-matter experts as possible in the brainstorming process can help mitigate this potential risk. As with many methodologies, this one depends entirely on the analyst to properly research the culture of the individual or group in question and accurately apply that research to come up with an appropriate attack.

¹⁵ A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis. Central Intelligence Agency. Vol. 2, No. 2. June 2005.

C.2.1. Devil's Advocacy Steps

Step 1: Identify and research a position that is completely contrary to the current best position

Part One (1-1): Determine the current position of the group or individual. Then determine what the most contradictory position could possibly be.

Part Two (1-2): Using any resources available, thoroughly research the contradictory position.

Step 2: Confront the group or individual with the new position

Using the research from step 1-2, create and present an argument for the contradictory position. Make sure to present the position as if the presenter is a firm believer in it

Step 3: Reassess all of the possible solutions to choose the best one

Review the list of possible solutions to the problem at hand. Given the new light in which the most popular solution is now shown, reassess which of the solutions is the best. The previously chosen solution may still be the best choice.

C.2.2. Illustrative Example

A team of analysts for a city on the Mississippi Coast are preparing an evacuation plan in case a hurricane is imminent and the residents need to be evacuated. Collectively, they decided that warning the population and issuing a command to evacuate via the highways would be the best way to clear the city. However, they arrived on this solution fairly quickly, and some of the analysts want to try a devil's advocate exercise to ensure that they have the right solution.

Step 1

The analysts determined that the current solution was to announce the impending emergency, and alert the public to evacuate on their own via the highway system. The analysts decided that another position would be to have the citizens stay in their homes until either the police or National Guard came and escorted them out of the danger area.

Step 2

After exhaustive research efforts, the devil's advocate team presented their argument to the analysts. They determined that an evacuation left to the people would be unorganized and lead to traffic jams, thus constricting the flow of people out of the danger area. They proposed that an organized evacuation, where one group at a time was escorted by either the local police or the National Guard out of the city would be more organized, lead to fewer traffic incidents and motor vehicle accidents, and speed up the evacuation process.

Step 3

The analysts then reassessed all of their solutions and decided that the initial plan was the fastest method of evacuating the most people. They rejected the devil's advocate position because setting up the evacuation and putting the National Guard in place would take too long.

C.3. DIVERGENT-CONVERGENT THINKING

What is it? Divergent-Convergent Thinking is a form of structured brainstorming that generates new analytic ideas, hypotheses, and concepts or helps discover previously unimagined hazards, vulnerabilities, and risky situations through an unconstrained creative group process.^{16, 17}

Why use it? For risk assessments, Divergent-Convergent Thinking can be used to:

- Identify the factors that influence the cause, magnitude, and extent of loss following a shock or incident.
 - Brainstorm potential ways in which an attacker can successfully inflict harm to an organization, jurisdiction, or region.
 - Imagine how response situations could be better or worse, relative to past experience.
 - Describe and categorize the hazards and vulnerabilities that are relevant to an organization, jurisdiction, or region.
 - Construct a fact-finding template for surveying sites, observation locations, and eliciting opinions.
-

Timing Divergent-Convergent Thinking can be used any time during the course of a risk study where creativity and imagination are necessary for high quality output. This technique works best when individuals come together as a group to develop multiple ideas, hypotheses, concepts, causal factors, considerations, etc.

¹⁶ A Tradecraft Primer: Basic Structured Analytic Techniques. Defense Intelligence Agency. March 2008, pp. 21-24.

¹⁷ Jones, Morgan D. *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving*. New York: Three Rivers, 1998. Print.

Steps	The overall approach for conducting a Divergent-Convergent Thinking exercise is comprised of five steps:
1.	Exercise Preparation
a.	Select participants
b.	Schedule meeting times
c.	Appoint a facilitator
d.	Provide materials
2.	Identify the Key Risk Question
a.	Discuss the topic and articulate an appropriate key risk
b.	Refine the question and gain group consensus
3.	Divergent Thinking
a.	Request responses
b.	Collect responses
c.	End the “collection stage”
4.	Convergent Thinking
a.	Rearrange ideas by commonalities or similar concepts
b.	Select a word or phrase that best characterizes each group
c.	Identify useless noise or an idea that deserves further attention
d.	Challenge the groupings and their composition
5.	Summary and Wrap-Up
a.	Discuss what was accomplished during this exercise
b.	Select one or two areas that deserve the most attention
c.	Discuss next steps for the group
d.	Summarize the results

Tips	This technique complements a number of other techniques, including:
	<ul style="list-style-type: none">• Reverse Brainstorming (Appendix C.6)• Premortem Analysis (Appendix P)• Developing Factor-Based Models (Appendix E)

Helps overcome biases. Divergent-Convergent Thinking can maximize an analyst or group effort to overcome individual biases. During the course of the activity, the process exposes external factors potentially affecting individual beliefs and may suggest new or larger issues that must be addressed.

Creative thinking and the reevaluation of mindsets and beliefs occur as new ideas are considered, unknown issues come to the fore, and existing ideas, hypotheses, and concepts are reexamined.

Promotes higher quality analysis. This technique enables groups to make explicit their reasons for coming to certain conclusions (e.g., assessment of risk, investment decisions). Making reasons explicit exposes them to criticism from peers, leadership and constituents, which in turn promotes higher quality analysis.

Participants learn from each other. This technique is a simple and quick way for participating experts to come together to learn from each other. During the process, each participant has the opportunity to share what they know; accordingly, other participants may discover what they don't fully know and how their expertise differs from the others.

All ideas are welcome. This technique provides a means for all participants to bring forward their ideas without the fear of criticism.

Susceptibility to bias. Group members are very susceptible to anchoring bias. Their creativity is often constrained by their past experiences or immediate experiences of others. Encourage those less susceptible to anchoring bias to help others break free of their past experiences to imagine the full-range of possibilities.

Negative reactions to ideas. One negative comment or gesture can shut down the creativity of the members of the group. It is important for the facilitator and other group members to promote, maintain, and guarantee freedom of expression throughout the process. One technique to mitigate this problem is to prohibit verbal or physical reactions to others' ideas.

Thinking out-loud. Analysts think much faster than they voice their thoughts, causing nonspeaking members to either forget an idea or to become frustrated. Both obstacles can be overcome to some degree by the use of Post-it notes and not allowing verbal or physical reaction to others' ideas.

C.3.1. Divergent-Convergent Thinking Steps

Exercise Preparation

The following preparation steps should be coordinated by a facilitator or dedicated study leader.

1. Select participants. In some cases the group composition is fixed and obvious. In other cases, care should be taken to select participants with complementary or contrasting experiences. It is often helpful to invite at least one person who is completely unfamiliar with the question of interest. Typically, a group of 5-12 participants works best; a larger or smaller group is not as effective.

2. Schedule time to conduct this activity face-to-face as a group at a mutually convenient time and location. All participants should attend. Anyone who does not attend should not be listed as a participant.
 - a. Plan on the activity taking about one hour to complete.
 - b. The Internet offers a number of inexpensive or free alternative ways of conducting a Divergent-Convergent Thinking exercise. Such alternatives include:
 - i. Online videoconferencing or web meeting space (e.g., Skype, Adobe Connect, GoToMeeting, WebEx, Microsoft Lync)
 - ii. Public virtual worlds (e.g., Second Life)
 - c. Use any room with a large, flat, empty surface that can accommodate sticky notes. A large white board works great for this purpose. If the sticky notes do not adhere to the surface well enough or for longer than a few minutes, consider taping a large sheet of paper to the wall to create a more adherent work surface.
3. Appoint as a facilitator or study leader – a person from the group that is familiar with the Divergent-Convergent Thinking process. The facilitator here acts as both participant AND process leader.
 - a. If resources permit, you may also dedicate an individual as solely the process leader; however, the dedicated process leader must maintain impartiality throughout and only make suggestions as necessary to spark creativity.
4. Provide sticky notes and markers, pens, or crayons to all participants. Make sure a variety of colors for both sticky notes and writing are available; it is common to organize thinking around certain colors, identifying contributor by color, or use the colors for a variety of ad hoc purposes.

Step 1: Identify the Key Risk Question

This initial phase establishes the key risk question or question at issue for the Divergent-Convergent Thinking activity.

Part One (1-1): Discuss the topic at issue and articulate an appropriate key risk question for the brainstorming exercise. Allow sufficient time for discussing the nuances of the question, to include the scope, definitions of key terms, assumptions, and so on.

Part Two (1-2): Refine the question as needed until the group achieves consensus on its meaning. (Note: The use of the Problem Restatement and Issue Development [[Appendix Q](#)] structured analysis technique may help with defining the best key risk question in Step 1 of this phase.)

Step 2: Divergent Thinking

The Divergent Thinking phase encourages participants to share and note all ideas that come to mind that relate to the key risk question or question at issue.

Part One (2-1): Ask the group to write down responses to the question. Each response should take the form of a short phrase or one to five keywords.

Part Two (2-2): For the first one or two rounds, have each participant in turn stand up and stick a response on the board. It often helps here to say the response out loud while sticking it to the board so others can hear and reflect on it. Do not allow others to criticize or discuss any of these ideas. However, do allow the participants to voluntarily clarify their response provided it is brief (a good rule of thumb is to allow participants to clarify their ideas only during the time spent transiting between their seat and the work surface).

Tip: Participants generally have a tendency to conserve space when writing their ideas down on a sticky note. Typically, this means that others need to squint and waste time trying to read and absorb the ideas of the conservationist. The time lost trying to read the small handwriting of others is often distracting and counterproductive. Encourage all participants to write big and bold and to not let any stick-note space go unused.

Part Three (2-3): When the time is right, allow all group members to stick as many additional responses to the board as they see fit. Treat all responses equally no matter how ridiculous they may seem – some of the most inspiring ideas often seem silly in isolation. Duplicates are also okay. It is helpful to insist that all participants stand up facing the work surface for the remainder of the Divergent Thinking phase.

Part Four (2-4): When a significant pause follows the initial flow of ideas, the group is reaching the end of their conventional thinking and the new divergent ideas are likely to emerge. If you see a group member slowing down in their responses, encourage him or her to take some time to read the other participants' responses to prompt this divergent thinking.

Part Five (2-5): End the “collection stage” of the brainstorming after two or three pauses. This point is typically referred to as the 80-20 point. At this point 80-percent of possible ideas were posted to the work surface in 20-percent of the time it would take to get all 100-percent. If efforts were taken to extract the remaining 20-percent, you will find that this last effort will take 80-percent of the total exercise time.

Step 3: Convergent Thinking

The Convergent Thinking phase encourage participants to work together to organize the multiple ideas into categories, groups, and collections of like concepts.

Part One (3-1): Ask participants as a group to rearrange the ideas on the wall according to their commonalities or similar concepts. Some notes may be moved several times as notes begin to cluster. Copying some notes is permitted to allow ideas to be included in more than one group. Other notes may not fit within any category or group. Sometimes it helps to limit talking among the participants during this step, though this is not required.

Participants are encouraged to add new ideas during the Convergent Thinking phase as needed. However, if the Divergent Thinking phase was performed well, the number of new ideas that appear in this later phase is generally limited in number.

Part Two (3-2): Once all of the ideas are organized, select a word or phrase that best characterizes each group. The appropriate label should be negotiated among all participants. The specific ideas comprising a group provide a nuanced definition.

Part Three (3-3): Identify any notes that do not easily fit with others and consider them either useless noise or the beginning of an idea that deserves further attention.

Part Four (3-4): Challenge the groupings and their composition. For example, as a group consider the following questions:

- What ideas are missing from a particular grouping?
- What groups should be broken down into two or more smaller or more specific groups?
- What groups should be consolidated into a larger group?
- What groups should be removed?

The results from this step should be used as appropriate to modify the groupings and their composition.

Step 4: Summary and Wrap-Up

This final phase reviews the groupings and supporting ideas in detail and summarizes the entire activity in report form.

Part One (4-1): As a group, discuss what has accomplished during this exercise. Focus on what new ideas or concepts have been identified and what new areas need more work or further brainstorming.

Part Two (4-2): Instruct each participant to select one or two areas that deserve the most attention. Discuss each participant's priority list as a group. It may be helpful to also ask each participant to list one or two areas that do not deserve attention. A variety of voting techniques may be helpful for this purpose.

Part Three (4-3): Discuss next steps for the group, to include future brainstorming sessions and upcoming analysis.

Part Four (4-4): Summarize the results from this session on a worksheet.

C.3.2. Illustrative Examples

The following examples illustrate the use of the Divergent-Convergent Thinking technique for a variety of risk analysis purposes.

Example 1: Safety During a Mass Evacuation Event¹⁸

This example focused on the following key risk question: *What are the factors that influence the safety of people during a rapid mass evacuation event?*

With the key risk question defined, discussed, and agreed upon, participants posted short keyword responses to the question to the wall. After each participant put out their initial ideas, the responses of others inspired participants to consider new, previously unconsidered or forgotten responses. This is the Divergent Thinking phase of the process. The Divergent Thinking phase continued until the group reached a point where few if any new ideas were posted.



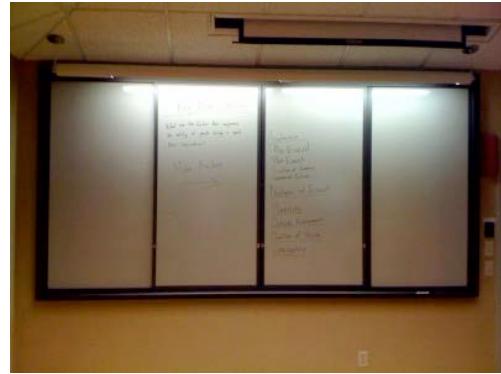
¹⁸ The session involved the participation of five undergraduate students from the Security Risk Analysis program at The Pennsylvania State University.

Given the large set of responses, the next phase sought to converge on a small set of general factors that influence the safety of individuals participating in a rapid mass evacuation. This was done by moving each individual response to a location on the wall associated with a group. We note that each response can belong to multiple groups – being mutually exclusive was not a requirement.

Once the groupings were established, each was reviewed by the participants to see if they made sense, were too general or too specific. In the end, each grouping is defined by its elements. This means that though a group may have a simple, vague label, its contents add clarity to what it specifically means to the group.

At the conclusion of this exercise, we had a listing of 9 factors thought by the group to be the key drivers influencing the safety of people during a rapid mass evacuation event. At this point, the process could have continued a bit further by having the group rank and sort the factors, vote for which of the 5-7 are most important, and so on.

In the end, the results from this Divergent-Convergent Thinking exercise were summarized in a simple worksheet that notes all responses, resulting groupings and results from any additional analysis (voting, ranking, etc.).



Example 2: Defining a Fact-Finding Template for Flood Monitoring Locations¹⁹

The aim of this study was to develop a fact-finding template for characterizing each of 14 flood monitoring sites within Centre County, Pennsylvania. The data collected at each one of these sites helps county officials predict the onset of floods and plan evacuations. Of particular interest were the characteristics of a site that affect the ability and quality of human observations (e.g., phone reporting).

The analysts supporting this activity were five graduate students at The Pennsylvania State University tasked with improving the flood warning system in Centre County. Based on a thorough discussion of the issue, the group focused on the following question at issue: *What aspects of a sensing location affect the precision, accuracy, reliability and sampling rate of a human sensor?*

Note that the particular wording of this question was negotiated using the Problem Restatement and Issue Development technique ([Appendix Q](#)). The decision to apply the Divergent-Convergent Thinking technique was made spontaneously based on the need for creativity and imagination in answering the question at issue.

¹⁹ The session involved the participation of five graduate students from the Information Sciences & Technology program at The Pennsylvania State University.

Once the participants settled on the question, they proceeded to brainstorm factors that shape the reliability of human reports (the Divergent Thinking phase). Sticky notes were used for posting ideas. The work surface used was a small-sized whiteboard (nearest available). This phase took about 30 minutes to complete and generated 105 responses:

3G service reliability and service flooding	Durability	Network accessibility	Sensor damaged?
Ability to read at night	Durability	Nighttime hazard	Sensor on pedestrian or automotive route
Accessibility	Ease of reading	No cellular or GPS coverage	Shifting of stream patterns
Age	Elevation	Number of volunteers	Soft versus hard sensor
Animals	Environment changes	Other civic works	Soil permeability
Any memorials for past human accidents/mishaps?	Erosion of the lakebed	Past events that changed stream morphology	Spawning routes
Are there variable/unwanted influences on sensors?	Graffiti	People's voluntariness	Stream characteristics
Awareness campaigns	Guidelines for volunteers	Perceptually safe for students	Stream grade
Broken? Torn?	Historical data/examples	Physical condition of yardstick	Stream significance
Businesses and schools	Honesty	Physical features (steep vs. gentle slope, deep vs. shallow)	Terrain
Can people find the sensor?	How easy could it be sabotaged or altered?	Plants/algae	Threatening residents
Civil restrictions	How often do people walk by?	Pollution of lakebed	Time of day
Consistency within/between volunteers	How often is data collected	Population/availability of volunteers	Time required to take measurement
Contaminated	Ice/weather manipulation	Presence of rabid ostriches	Understanding of the task
Contamination and pollution	Incentivizing participation	Proximity to game/hiking trails	Variability of the water table
Cost of human to do that and their incentives	Is the sensor easily located?	Proximity to game/hiking trails	Verification rate that it works & accurate
County population	Lighting and shadowing	Proximity to threats	Visible from shore (bank)

Danger of observing - will they fall into the stream?	Maintenance	Rate of variability	Volunteer demographic for soft sensors
Data collecting personnel	Maintenance	Representatives with respect to its domain	Volunteer recruitment methods in nearby cities
Data collection method	Marker is inaccurate	Response inter-reliability	Warning and notification signs
Data storage/trend analysis	Markers worn or illegible	Response time or lag period	Weather
Debris and animals	Monitoring of data for reasonableness	Safe	Whether or not personnel are stationed nearby
Differences between sensors	Monitoring of volunteers	Season	Who will read the sensor?
Distance to residences	Morphology	Sensitivity	Will reading have potential danger for the reader
Does the data shown differ when people look from different positions?	Motivation/compensation	Sensor calibration	Will the data be easily changed by humans or animals?
Will the data be wrongly used and cause unnecessary panic?			

The participants proceeded to group the ideas into categories (the Convergent Thinking phase). Labels for each category were noted using an erasable whiteboard marker.

This phase took about 20 minutes to complete and generated the following 6 categories:

- Geography
- People / Animals
- History
- Sensor Staff
- Physical Condition of Sensors
- Sensor Technology

This page is intentionally blank.

C.3.a. CIA Approach to Divergent-Convergent Thinking

What is it? The following describes the Divergent-Convergent Thinking approach described in the Central Intelligence Agency (CIA) Tradecraft Primer.²⁰ Divergent-Convergent Thinking is a form of structured brainstorming that generates new analytic ideas, hypotheses and concepts or helps discover previously unimagined hazards, vulnerabilities and risky situations through an unconstrained creative group process.

Why use it? **Helps overcome biases.** Divergent-Convergent Thinking can maximize an analyst or group effort to overcome individual biases. During the course of the activity, the process exposes external factors potentially affecting individual beliefs and may suggest new or larger issues that must be addressed. Creative thinking and the reevaluation of mindsets and beliefs occur as new ideas are considered, unknown issues come to the fore, and existing ideas, hypotheses, and concepts are reexamined.

Promotes higher quality analysis. This technique enables groups to make explicit their reasons for coming to certain conclusions (e.g., assessment of risk, investment decisions). Making reasons explicit exposes them to criticism from peers, leadership and constituents, which in turn promotes higher quality analysis.

Participants learn from each other. This technique is a simple and quick way for participating experts to come together to learn from each other. During the process, each participant has the opportunity to share what they know; accordingly, other participants may discover what they don't fully know and how their expertise differs from the others.

All ideas are welcome. This technique provides a means for all participants to bring forward their ideas without the fear of criticism.

²⁰ A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis. Central Intelligence Agency. Vol. 2, No. 2. June 2005, pp. 29-31.

Timing Divergent-Convergent Thinking can be used either at any time during the course of a risk study where creativity and imagination are necessary for high quality output. This technique works best when individuals come together as a group to develop multiple ideas, hypotheses, concepts, causal factors, considerations, etc. For risk assessment, Divergent-Convergent Thinking can be used to:

- Identify the factors that influence the cause, magnitude and extent of loss following a shock or incident
- Brainstorm potential ways in which an attacker can successfully inflict harm to an organization, jurisdiction, or region
- Imagine how response situations could be better or worse relative to past experience
- Describe and categorize the hazards and vulnerabilities that are relevant to an organization, jurisdiction, or region
- Construct a fact-finding template for surveying sites, observation locations, and eliciting opinions

This technique complements a number of other techniques, including:

- Reverse Brainstorming ([Appendix C.6](#))
- Premortem Analysis ([Appendix P](#))
- Developing Factor-Based Models ([Appendix E](#))

Steps

The method below consists of two steps:

1. Divergent Thinking
2. Convergent Thinking

The method presumes that a key risk question has been identified prior to commencing this brainstorming exercise.

Step 1: Divergent Thinking

Part One (1-1): Distribute post-it notes and pens or markers to all participants.

Typically, 10-12 people works best.

Part Two (1-2): Pose the problem in terms of a “focal question.” Display it in one sentence on a large easel or whiteboard.

Part Three (1-3): Ask the group to write down responses to the question, using keywords that will fit on the small post-it note.

Part Four (1-4): Stick all the notes on the wall for all to see - treat all ideas the same.

Part Five (1-5): When a pause follows the initial flow of ideas, the group is reaching the end of their conventional thinking and the new divergent ideas are likely to emerge.

Part Six (1-6): End the “collection stage” of the brainstorming after two or three pauses.

Step 2: Convergent Thinking

Part One (2-1): Ask participants as a group to rearrange the notes on the wall according to their commonalities or similar concepts. No talking is permitted. Some notes may be moved several times as notes begin to cluster. Copying some notes is permitted to allow ideas to be included in more than one group.

Part Two (2-2): Select a word or phrase that characterizes each grouping or cluster once all the notes have been arranged.

Part Three (2-3): Identify any notes that do not easily fit with others and consider them either useless noise or the beginning of an idea that deserves further attention.

Part Four (2-4): Assess what the group has accomplished in terms of new ideas or concepts identified or new areas that need more work or further brainstorming.

Part Five (2-5): Instruct each participant to select one or two areas that deserve the most attention. Tabulate the votes.

Part Six (2-6): Set the brainstorming group’s priorities based on the voting and decide on the next steps for analysis.

Tips

Susceptibility to bias. Group members are very susceptible to anchoring bias. Their creativity is often constrained by their past experiences or immediate experiences of others. Encourage those less susceptible to anchoring bias to help others break free of their past experiences to imagine the full-range of possibilities.

Negative reactions to ideas. One negative comment or gesture can shut down the creativity of the members of the group. It is important for the facilitator and other group members to promote, maintain, and guarantee freedom of expression throughout the process. One technique to mitigate this problem is to prohibit verbal or physical reactions to others' ideas.

Thinking out-loud. Analysts think much faster than they voice their thoughts, causing nonspeaking members to either forget an idea or to become frustrated. Both obstacles can be overcome to some degree by the use of Post-it notes and not allowing verbal or physical reaction to others' ideas.

This page is intentionally blank.

C.3.b. DIA Approach to Divergent-Convergent Thinking

What is it? The following describes the Divergent-Convergent Thinking approach described in the Defense Intelligence Agency tradecraft primer.²¹ Divergent-Convergent Thinking is a form of structured brainstorming that generates new analytic ideas, hypotheses and concepts or helps discover previously unimagined hazards, vulnerabilities and risky situations through an unconstrained creative group process.

Why use it? **Helps overcome biases.** Divergent-Convergent Thinking can maximize an analyst or group effort to overcome individual biases. During the course of the activity, the process exposes external factors potentially affecting individual beliefs and may suggest new or larger issues that must be addressed. Creative thinking and the reevaluation of mindsets and beliefs occur as new ideas are considered, unknown issues come to the fore, and existing ideas, hypotheses, and concepts are reexamined.

Promotes higher quality analysis. This technique enables groups to make explicit their reasons for coming to certain conclusions (e.g., assessment of risk, investment decisions). Making reasons explicit exposes them to criticism from peers, leadership and constituents, which in turn promotes higher quality analysis.

Participants learn from each other. This technique is a simple and quick way for participating experts to come together to learn from each other. During the process, each participant has the opportunity to share what they know; accordingly, other participants may discover what they don't fully know and how their expertise differs from the others.

All ideas are welcome. This technique provides a means for all participants to bring forward their ideas without the fear of criticism.

²¹ *A Tradecraft Primer: Basic Structured Analytic Techniques*. Defense Intelligence Agency. March 2008, pp. 21-24.

Timing

Divergent-Convergent Thinking can be used either at any time during the course of a risk study where creativity and imagination are necessary for high quality output. This technique works best when individuals come together as a group to develop multiple ideas, hypotheses, concepts, causal factors, considerations, etc. For risk assessment, Divergent-Convergent Thinking can be used to:

- Identify the factors that influence the cause, magnitude and extent of loss following a shock or incident
- Brainstorm potential ways in which an attacker can successfully inflict harm to an organization, jurisdiction, or region
- Imagine how response situations could be better or worse relative to past experience
- Describe and categorize the hazards and vulnerabilities that are relevant to an organization, jurisdiction, or region
- Construct a fact-finding template for surveying sites, observation locations and eliciting opinions

This technique complements a number of other techniques, including:

- Reverse Brainstorming ([Appendix C.6](#))
- Premortem Analysis ([Appendix P](#))
- Developing Factor-Based Models ([Appendix E](#))

Steps

The method below consists of two steps:

1. Divergent Thinking
2. Convergent Thinking

The method presumes that a key risk question has been identified prior to commencing this brainstorming exercise.

Step 1: Divergent Thinking

Part One (1-1): Organize the group. Group members should come from a variety of backgrounds (cross fertilization is important). Cognitive diversity, different points of view, and a wide range of experience are important. Small groups tend to function better than large ones; five to seven participants is a good target.

Part Two (1-2): Focus on a specific topic or question. It should not be so broad that no solution is possible or so narrow that creativity won't help. Make clear to all members in advance that discussion will not be constrained by current positions or available evidence.

Part Three (1-3): Have everyone write down at least one idea before discussion starts. Use paper, white boards, or Post-it notes to record ideas. That will allow easy clustering of ideas during the Convergent Thinking phase.

Part Four (1-4): Have the group verbally generate as many ideas as possible. When a group has one or more strong personalities, the facilitator can have the members stop all verbalization and write their ideas down and post them where others can read them and build on any idea. Listen closely as others talk; this will help generate ideas. Suspend judgment; do not eliminate ideas; what looks crazy at first may become valuable later, after more thought or when new data is received.

Part Five (1-5): Let the first session last for 45-60 minutes or until a noticeable decline in activity takes place. Then take a break. Keep going for two more sessions, ending each when the activity falls off. After the third such period, it is time to stop the Divergent Thinking phase.

Step 2: Convergent Thinking

Part One (2-1): Group the ideas by theme, then set aside any that do not easily fit with any group. Then through voting or other means, select the themes or outliers that deserve further attention.

Part Two (2-2): After the session is over, have the individuals spend time alone to silently review the submission and consider:

- For Benefit-Cost Analysis: Which of the alternatives are reasonable and would meet the goals of the decision maker?
- For threat identification: Which of the alternatives are plausible and warrant further study?
- For any question: what additional analysis is needed and what is the associated expected value of information?

Tips

Susceptibility to bias. Group members are very susceptible to anchoring bias. Their creativity is often constrained by their past experiences or immediate experiences of others. Encourage those less susceptible to anchoring bias to help others break free of their past experiences to imagine the full-range of possibilities.

Negative reactions to ideas. One negative comment or gesture can shut down the creativity of the members of the group. It is important for the facilitator and other group members to promote, maintain and guarantee freedom of expression throughout the process. One technique to mitigate this problem is to prohibit verbal or physical reactions to others' ideas.

Thinking out-loud. Analysts think much faster than they voice their thoughts, causing nonspeaking members to either forget an idea or to become frustrated. Both obstacles can be overcome to some degree by the use of Post-it notes and not allowing verbal or physical reaction to others' ideas.

This page is intentionally blank.

C.4. OUTSIDE-IN THINKING

What is it? Outside-In Thinking is used to identify the full range of basic forces, factors, and trends that would indirectly shape an issue.²² Outside-In Thinking is one of a variety of brainstorming techniques.

Why use it? Most analysts spend their time concentrating on familiar factors within their field or analytic issue. That is, they think from the “inside”—namely, what they control—out to the broader world. Conversely, “thinking from the outside-in” begins by considering the external changes that might, over time, profoundly affect the analysts’ own field or issue. This technique encourages analysts to get away from their immediate analytic tasks (the so-called “inbox”) and think about their issues in a wider conceptual and contextual framework.

By recasting the problem in much broader and fundamental terms, analysts are more likely to uncover additional factors, an important dynamic, or a relevant alternative hypothesis.

Timing Analysts find this technique most useful at the conceptualization of an analytic project, when the goal is to identify all the critical, external factors that could influence how a particular situation will develop. It would work well for a group of analysts responsible for a range of functional and/or localized issues. When assembling a large database that must identify a number of information categories or database fields, this technique can aid in visualizing the entire set of categories that might be needed in a research effort. Often analysts realize only too late that some additional information categories will be needed and then must go back and review all previous files and recode the data. With a modest amount of effort, Outside-In Thinking can reduce the risk of missing important variables early in the analytic process.

Steps The process begins by developing a generic description of the problem or the phenomenon under study. Then, analysts should:

Step 1: List all the key forces (social, technological, economic, environmental, and political) that could have an impact on the topic, but over which one can exert little influence (e.g., globalization, social stress, the Internet, or the global economy).

Step 2: Focus next on key factors over which an actor or policymaker can exert some influence. In the business world this might be the market size, customers, the competition, suppliers or partners; in the government domain it might include the policy actions or the behavior of allies or adversaries.

Step 3: Assess how each of these forces could affect the analytic problem.

Step 4: Determine whether these forces actually do have an impact on the particular issue based on the available evidence.

²² *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*. Central Intelligence Agency. Vol. 2, No. 2, June 2005, pp. 29-31.

This page is intentionally blank.

C.5. ROUND-ROBIN BRAINSTORMING

What is it? Like many brainstorming techniques, Round-Robin Brainstorming relies on ideas being generated in the absence of discussion for completely free-form thoughts unhindered by group trends or consensus.²³

Why use it? Your group uses other people's ideas to generate even more ideas, without being influenced by assertive or vocal members of the team. Another advantage of this approach is that it also ensures that everyone in your group gets an equal chance to present their ideas. If your team has shy or low-confidence members, this method can help them feel more comfortable.

Timing Round-Robin Brainstorming is a useful tool for having your team generate ideas, without being influenced unduly by others in the group. This method also ensures that everyone on your team has an equal say in the ideas that you generate. You can use either the written and verbal variations of this technique.

Steps The Round-Robin Brainstorming technique consists of the following six steps:

Step 1: Set your group or team around a table. Give each one a stack of index cards.

Step 2: The problem or issue at hand is explained by the facilitator. If people want to discuss their ideas, stop them. (This may not be easy.) The important thing is not to "taint" their creativity with only one or two threads that might stifle new ideas.

Step 3: In relative silence, each person takes a card and writes down one idea. He or she then passes the card to the person on the right.

Step 4: That person reads the card and uses it to generate a new idea. He or she then turns the first card upside down in a stack, and passes the new card to the right.

Step 5: The process of writing new ideas and passing to the person on the right continues for a set amount of time, perhaps ten minutes.

Step 6: At the end, the facilitator gathers the cards. Each idea is read aloud, and the cards are then arranged and grouped on a whiteboard or wall, with duplicates discarded. This is used to stimulate discussion or more ideas, preferably on another whiteboard or some mind-mapping software on a projector.

²³ Johnston, Douglas. "Round-Robin Brainstorming." *DIY Planner*. 24 November 2005. Web. <<http://www.diypalanner.com/node/411>>.

Tips

A disadvantage of Round-Robin Brainstorming is that it isn't anonymous. When team members pass ideas around the room, they might hold back simply because they know that the person next to them will see what they have written. Another disadvantage is that each person gets inspiration for their new idea from the ideas of only one other person, rather than from the entire group.

- You can make Round-Robin Brainstorming anonymous by gathering the ideas at each stage, shuffling them, and then passing them out again; rather than having group members pass their ideas to the person next to them.
- You can also use Round-Robin Brainstorming with larger groups. Divide everyone into smaller groups, and have each group develop one great idea and write it on an index card. Then, rotate cards between groups, just as you would with the individual variation. You then have each group brainstorm a new idea based on the previous group's card.²⁴

²⁴ "Round-Robin Brainstorming." Myself Space. 1 December 2010.
<<http://myselfspace.net/blogs/jerryjohn/archive/2010/12/01/2970.aspx>>.

C.6. REVERSE BRAINSTORMING

What is it? Reverse Brainstorming is a structured brainstorming technique that asks how and why a hazard might not occur, and uses the converse of these reasons to suggest how it might actually occur. Reverse brainstorming is a good technique for creative problem solving, and can lead to robust solutions. Be sure to follow the basic rules of brainstorming to explore possible solutions to the full.

Why use it? Reverse brainstorming helps you solve problems by combining brainstorming and reversal techniques. By combining these, you can extend your use of brainstorming to draw out even more creative ideas.

Timing To use this technique, you start with one of two “reverse” questions:

- Instead of asking, “How do I solve or prevent this problem?” ask, “How could I possibly cause the problem?”
- Instead of asking “How do I achieve these results?” ask, “How could I possibly achieve the opposite effect?”

Steps²⁵ The Reverse Brainstorming technique is comprised of the following five steps:
Step 1: Clearly identify the key risk question, and write it down for everyone to see. For reverse brainstorming, it is best to restate the question in the positive direction. For example, instead of:

- What factors influence the chances of death in a car accident?
- How effective is a particular countermeasure at mitigating risk?

You might recast it in a positive light as:

- Under what circumstances would an individual survive a car accident?
- Why is the particular countermeasure effective at mitigating risk?

Step 2: Reverse the problem or challenge by asking:

- How could I possibly cause the problem?”, or
- How could I possibly achieve the opposite effect?”

Step 3: Brainstorm the reverse problem to generate reverse solution ideas. Allow the brainstorm ideas to flow freely. Do not reject anything at this stage.
Step 4: Once you have brainstormed all the ideas to solve the reverse problem, now reverse these into solution ideas for the original problem or challenge.
Step 5: Evaluate these solution ideas. Can you see a potential solution? Can you see attributes of a potential solution?

²⁵ “Reverse Brainstorming.” Mind Tools. n.d. Web. <http://www.mindtools.com/pages/article/newCT_96.htm>.

C.6.1. Illustrative Example

Consider the key risk question: *What behaviors decrease the attractiveness of an individual (businessman in particular) to terrorists?*

For reverse brainstorming, we consider the inverse question: *What behaviors increase the attractiveness of an individual (a businessman in particular) to terrorists?*

From this starting point, a group of security-minded individuals might construct the following list:²⁶

- Make it easy for them to find you. Put your name on the mailbox and the front door.
- Make sure your home phone number is publicly listed and outside phone wires are easy to locate and cut.
- Pass the word around and impress all you meet casually as well as neighbors and friends that you have a very high, important position in a multi-national company.
- Frequently post your activities on social media sites. No such thing as too much information from your perspective.
- Get into the newspaper social columns as often as possible and have your picture included.
- Stick to your daily pattern and never vary your routine and ask your family to do likewise.
- Punctually, go for your 7:00 a.m. jog, never deviating the hour or usual course.
- Show your name or initials on your automobile license plate.
- Always park your car in the same space, especially when your name and title are designated.
- Never discuss personal security with your family or business associates. Keep them guessing.
- Don't protect your home with alarms, panic buttons, or general security protection devices. It may be more exciting to pay ransom.
- At the office, as at home, don't consider protection devices such as alarm, panic button, etc. – just have your secretary's office separate you from any stranger entering the office.
- Just toss away important and confidential business letters and/or documents – especially your travel plans and the profit and loss statement of subsidiary companies – why go through the trouble of tearing them up or using a shredding machine?
- Ignore any threatening letters or phone calls you or your company may receive.
- Pay no attention to bomb threats at your office or home.
- Don't plan for any emergencies that may arise, such as bombings, kidnappings, hostage situations, vandalism or sabotage. You're immune... nothing will ever happen.
- Don't pay attention when you see strangers driving past your home for days on end noting the schedules you and your family keep.
- Be a nice guy, pick up hitchhikers, especially on your way to work and when returning home.

²⁶ Strauss, Sheryl. *Security Problems in a Modern Society*. Boston: Butterworth, 1980. Print.

- Accept an invitation to meet with strangers at a secluded or unknown location.
- Don't inform yourself well in advance about the political climate of each country you are to go to.
- Tell everyone you contact about your travel schedule and itinerary well ahead of time.
- If traveling in your corporate jet, make sure the corporation name is indicated on the tail of the plane. Leave your aircraft unguarded during night hours.
- Reserve the finest suite in the hotel in your corporation's name and your name and title.
- Leave your corporation's confidential documents unprotected in your suite.
- Pass the word that your company has sufficient funds to pay a million dollars in commissions to the right people in order to sell your products better.
- At restaurants, give your name, title, and corporation name and make reservations well in advance.
- Don't warn your wife against shopping alone and visiting the different shopping centers alone.
- If terrorists kidnap or abduct you, be a hero and resist. Fight tooth-for-tooth even though you are outnumbered, out-skilled, and they carry machine guns.
- Tell your abductors that everything will be done to meet their demands and that you are a very important person.
- Keep your mind a blank! Don't notice the physical appearance of your abductors – tall, short, thin, obese, the way they speak, accents, identifying marks, clothing or shoes.
- If blindfolded, try not to pay attention to your surroundings. Ignore traffic patterns, sounds of birds, dogs, church bells, children, city sounds, country sounds, etc. Try not to notice going up hills or around corners, etc., because you might be able later to assist in locating the hideout and help recover the ransom that was paid.

From here, we systematically review each idea and take the inverse. The results are factors that relate to the initial question.

This page is intentionally blank.

APPENDIX D. CAUSE AND EFFECT DIAGRAMS

What is it? A Cause and Effect Diagram, also called a Fishbone Diagram or an Ishikawa Diagram, is a visual representation of possible contributing factors to an outcome of concern. The method was created by Professor Kaoru Ishikawa in 1943 to help workers at the Kawasaki Steel Works understand how a large set of factors could lead to an undesirable outcome.

Why use it? This methodology was designed to be an easy way to quickly identify the key contributing areas to a given outcome of concern, reveal the underlying factors for those areas, and then display them in an easily understood manner. Like a Hierarchical Holographic Model ([Appendix L](#)), the diagram displays information in terms of grouped sets of factors within a common area, allowing an analyst to quickly identify general areas in which issues may occur, and allowing the problem to be broken down for further analysis and mitigation.

Timing Assess Phase: The Cause and Effect Diagram is designed to assist in the process of brainstorming contributing factors to a given outcome of concern. This lends the methodology to easy application during a Premortem Analysis ([Appendix P](#)), as well as after an incident has occurred to illustrate the possible contributing factors to that incident so that they can be avoided in the future.

Steps The overall approach for constructing a Cause and Effect Diagram is comprised of four steps:

1. Define the scope and outcome of concern
2. Identify the possible contributing areas
3. Identify the factors within the contributing areas which cause the outcome of concern
4. Review the diagram

Tips This system is designed to assist in generating as complete a collection of contributing factors as possible. However, it does not ensure all possibilities are accounted for. Also, if this methodology is performed with a group of uninformed or under-informed individuals, the results may not be accurate. A Cause and Effect Diagram does not necessarily produce a complete set of possible factors. The Diagram's completion level is limited by the knowledge and imagination of the people involved in the process. Therefore, this methodology should be used with a group of knowledgeable people and a facilitator who has practiced this technique before. The Expert-Opinion Elicitation Process ([Appendix H](#)) may assist in identifying the right people and facilitator.

D.1. CAUSE AND EFFECT DIAGRAMS STEPS

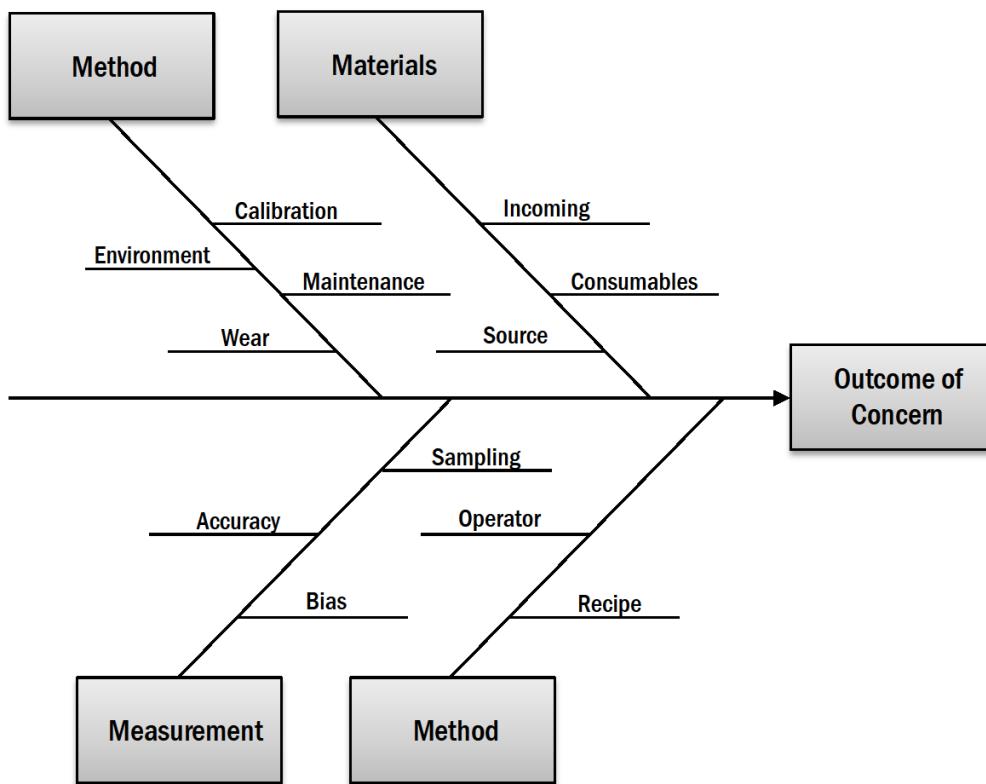
Step 1: Define the scope and outcome of concern

Part One (1-1): Define the scope of the exercise. Clearly state the system that is being examined, as well as the people, processes or equipment used within that system.

Part Two (1-2): Define the outcome of concern. Within the already defined system, detail the negative outcome you wish to avoid. Place that outcome in a box on the right hand side of the paper or chalkboard.

Step 2: Identify the possible contributing factors

Part One (2-1): Draw an arrow from left to right, pointing at the box with the outcome of concern. If you have a group of people, encourage them to call out possible categories of factors that would contribute to that negative outcome. One approach that would aid in doing this is Divergent-Convergent Thinking ([Appendix C.3](#)). If you do not have a group, you may do this alone. Typically used categories include Management, Manpower, Machines, and Materials (also known as the “4 M’s”); Place, Procedure, People, and Policies; and Surroundings, Suppliers, Systems, and Skills. Place each category in its own box along this line, and draw an arrow to the larger arrow you just drew. A schematic of a simple Cause and Effect Diagram is shown below.²⁷



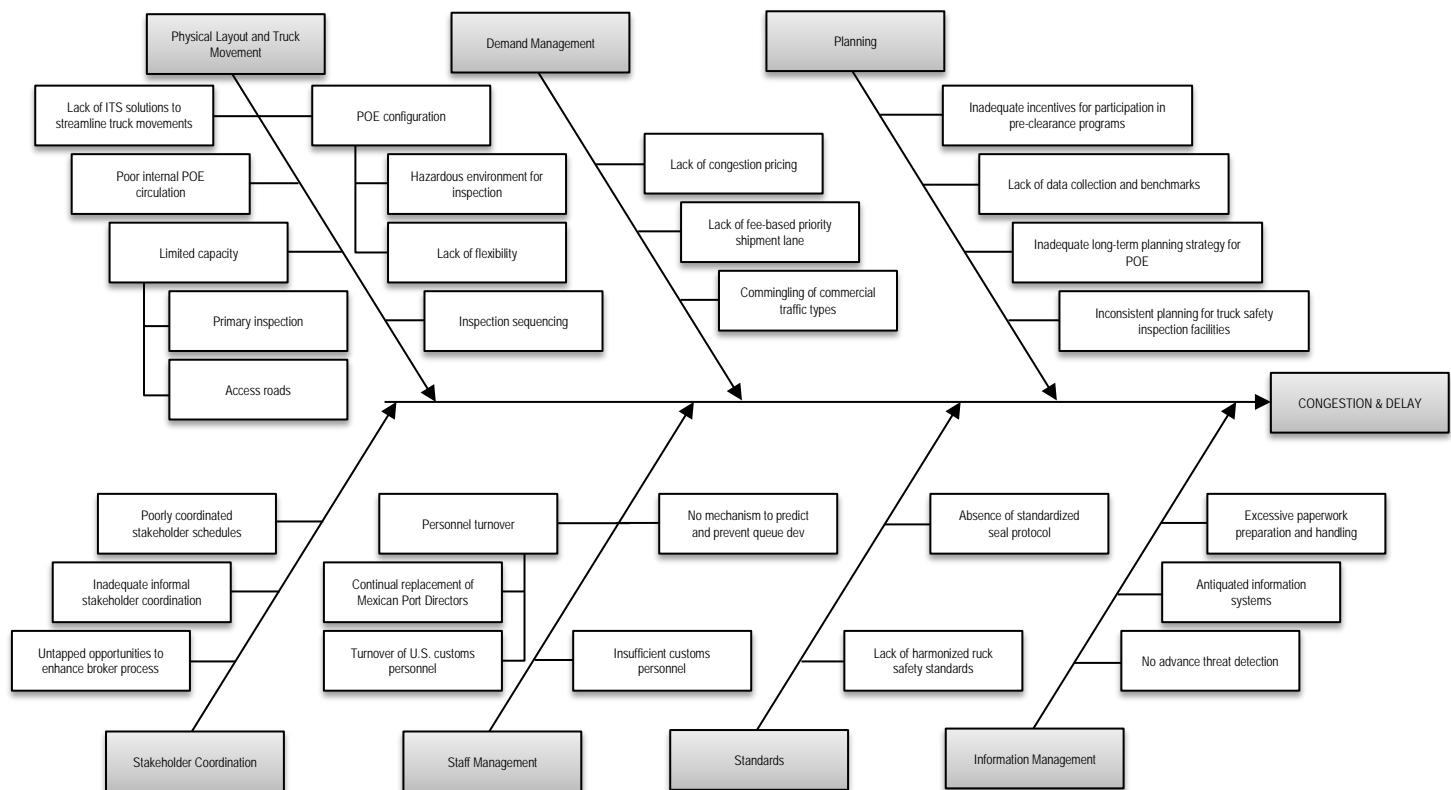
Part Two (2-2): Review the categories to ensure that there is as little overlap as possible. Also, see if there are any categories that have been missed.

²⁷ Digital image. Information Technology Laboratory, National Institute of Standards and Technology. n.d. Web. <<http://www.itl.nist.gov/div898/handbook/ppc/section1/gifs/img1352.gif>>.

Step 3: Identify the factors within the contributing areas that cause the outcome of concern

Part One (3-1): For each identified category or contributing area, brainstorm possible factors that would lead (individually or collectively) to the outcome of concern. Divergent-Convergent Thinking ([Appendix C.3](#)) exercises would be appropriate, but are not required.

Part Two (3-2): For each identified factor, consider if there are sub-factors which contribute to the factor and are within the scope of the exercise. Continue investigating each subsequent level of factors until they cannot be broken down or followed any further. A completed example of a Cause and Effect Diagram for a traffic coordination system through a border point of entry is shown below.²⁸



Part Three (3-3): Review the factors to ensure that the list generated is complete, and whether there are any factors which could be applied to other categories or contributing areas.

Step 4: Review the diagram

Part One (4-1): Review the entire document to ensure that it is complete and accurate. Make any adjustments as necessary.

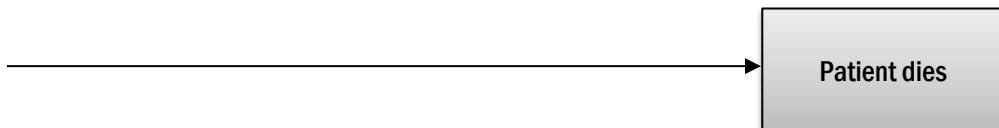
²⁸ Ojah, Mark I., Juan C. Villa, and William R. Stockton. "Truck Transportation through Border Points of Entry: Analysis of Coordination Systems." *US/Mexico Border Transportation Planning - FHWA*. November 2002. Web. <http://www.borderplanning.fhwa.dot.gov/TTIstudy/FOA_english.htm>.

D.2. ILLUSTRATIVE EXAMPLE

The following example constructs a Cause and Effect Diagram relating to patient mortality in a prehospital environment.

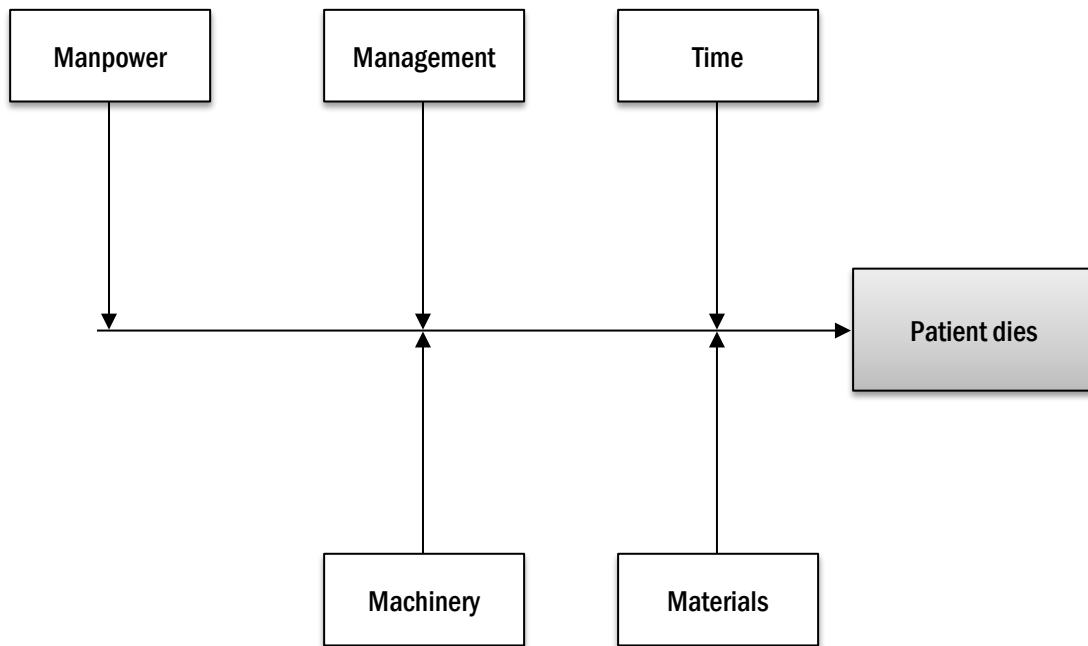
Step 1: Define the scope and outcome of concern

For this exercise, we will be examining the Emergency Medical System (EMS) in the United States. Specifically, we will be focusing on the network of emergency medical technicians (EMTs) and paramedics who respond to medical emergencies, their standard lifesaving equipment, and their vehicles. For this exercise, we will be considering only Type 3 ambulances, the specialized vehicles with an integrated cab and patient compartment. We will also only be considering EMT-Basic personnel, so basic life saving-only units. As with all patient care in the prehospital environment, the ultimate outcome of concern is that the patient lapses into irreversible shock and dies.



Step 2: Identify the possible contributing factors

The most common groupings for this exercise are the 4 M's: Management, Manpower, Machinery and Materials. Therefore, we are going to start with those four categories, as they conveniently fit this situation. However, we are going to add "Time" as well, as time is a major factor in EMS situations.



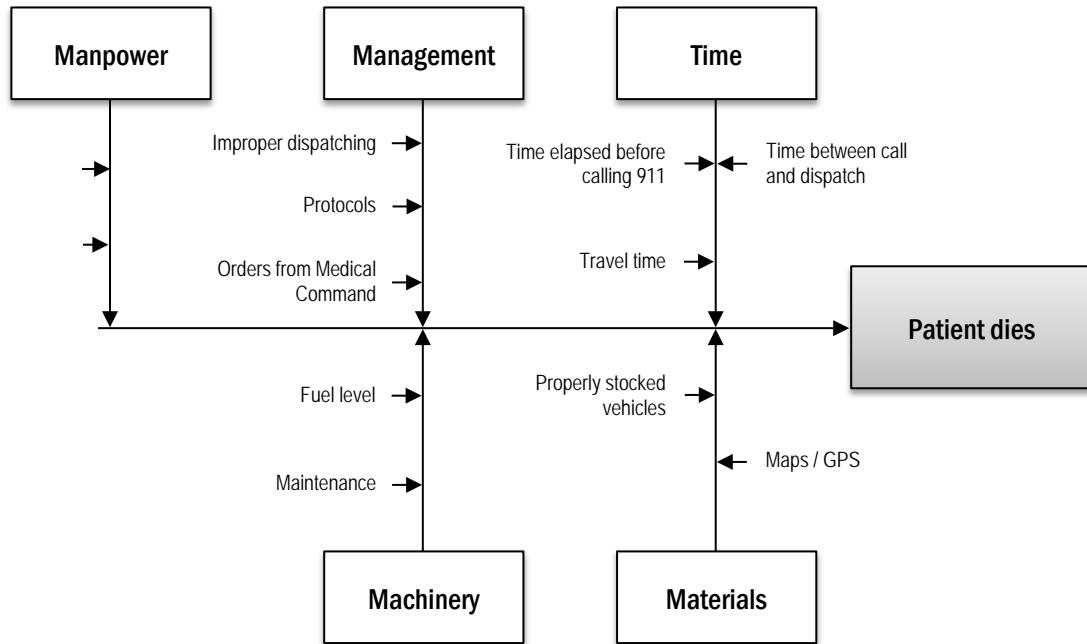
After reviewing the categories, we have determined that these will be sufficient to start the process.

Step 3: Identify the factors within the contributing areas that cause the outcome of concern

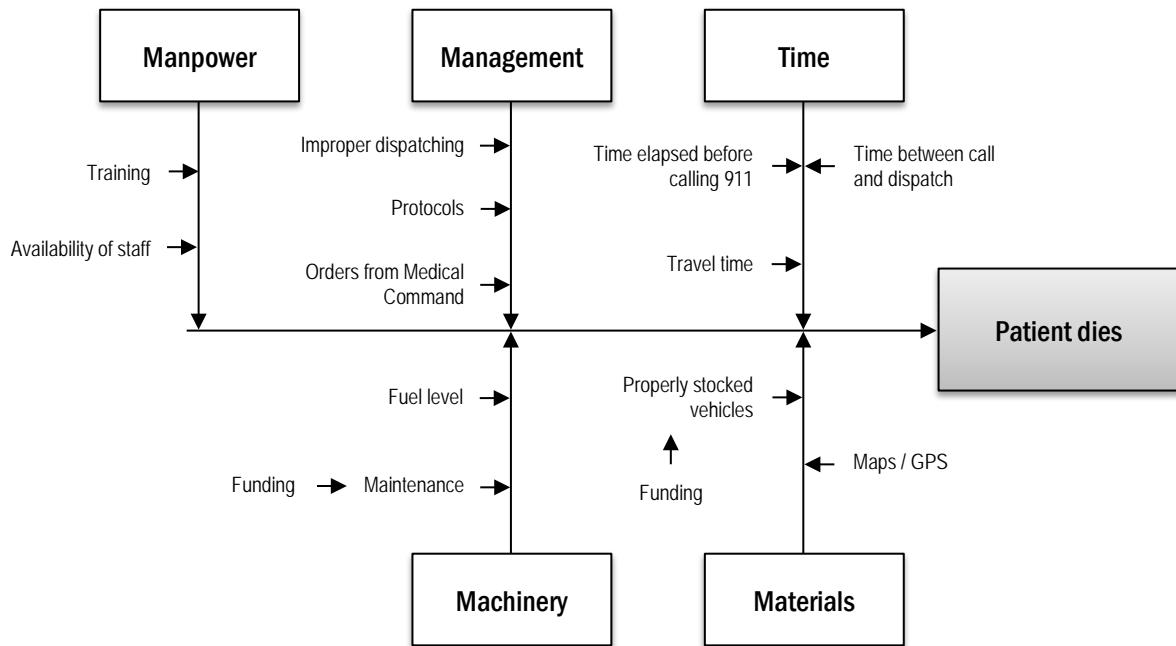
Working in a clockwise motion, the group started coming up with factors within each category. These factors included:

- Manpower
 - Training
 - Availability of staff
- Management
 - Improper dispatching
 - Bad protocols
 - Bad orders from medical command
- Time
 - Travel time
 - Time elapsed before calling 911
 - Time between call and dispatch
- Materials
 - AED availability
 - Properly stocked vehicles
 - Maps / GPS
- Machinery
 - Fuel level
 - Ambulance maintenance

The group then reviewed the factors to see if any could be added or if there were any redundancies. It was determined that “AED availability” was redundant with “Properly stocked vehicles,” so they were combined with a note to investigate AED availability as a sub-factor during the next step.



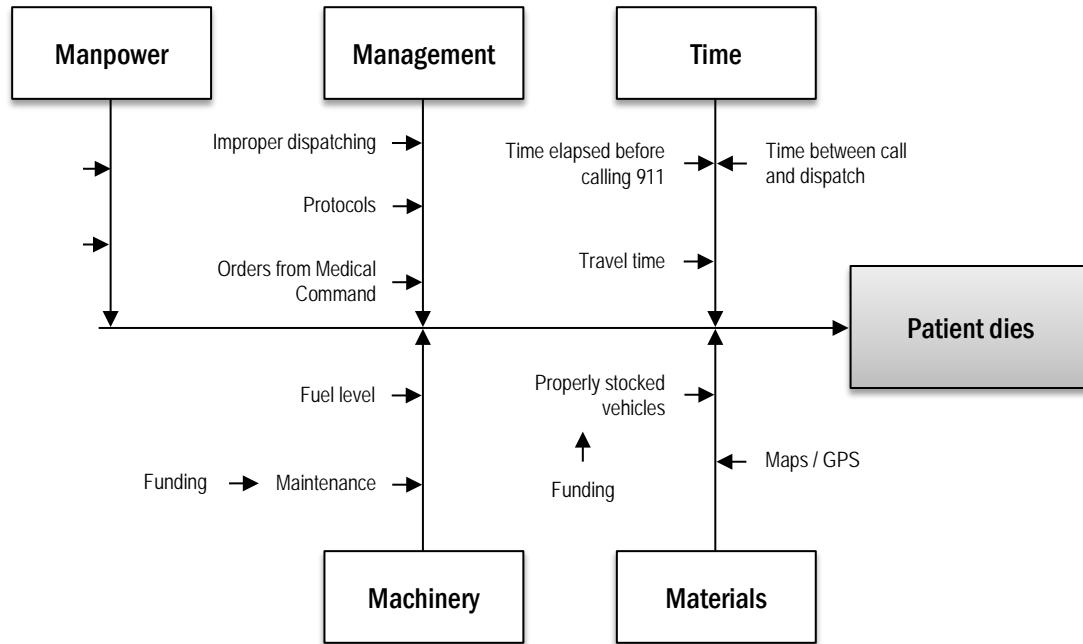
The next step is to determine the sub-factors, or whether there are any contributing factors to the ones we already identified. In identifying sub-factors, we identified that funding can cause maintenance issues, as well as lead to improperly stocked vehicles. Therefore, we added that sub-factor to those categories.



The group then reviewed the factors and decided that, within the scope of the exercise, the diagram was complete.

Step 4: Review the diagram

The group then reviewed the diagram as a whole and decided that, within the scope of the exercise, the diagram is complete. The group made sure to record the diagram and send it to all the participants for their final review later.



APPENDIX E. DEVELOPING FACTOR-BASED MODELS

What is it? This appendix provides guidance on developing or creating factor-based models. In general there are two types of factor-based models:

- V-Type or “Value-Type:” Models that describe low-level value dimensions (the factors) that relate in some way to higher-level values (the output). Models of this type might focus on assessing attractiveness of targets, place value on outcomes and establish rank-order preferences for countermeasures.
- F-Type or “Function-Type:” Models that describe predictor variables or state variables (the factors) that relate to some sort of response variable (the output). Models of this type presume a functional relationship between the factors and the outputs.

Factor-based models are a major part of Qualitative Risk Analysis, where the factors provide the means for breaking down complex problems into more manageable pieces.

Why use it? The process of creating a factor-based model generates new insights into the underlying relationships and influences affecting the answer or outcome to a given problem or question of interest.

Factor-based models also provide a template for analysis that is transparent for the consumer. To attain the necessary level of transparency, however, requires the analyst to fully document the model, to include a clear statement of the key risk question, baseline assumptions and specifics of the context surrounding the question, clear definitions of each factor and guidance on their assessment.

Timing Factor-based models are best used when a problem is poorly understood or difficult to answer in its raw form.

Steps The methodology for developing factor-based models is comprised of the following five steps:

1. Define and discuss the key risk question
2. Articulate all baseline assumptions and specifics of the problem context
3. Identify all relevant factors and document their specific meaning
4. Suggest how factors interact to generate outcomes or outputs
5. Describe under what circumstances this model may not be appropriate and identify alternative points of view

- Tips**
- A model is only as good as the information and expertise used to create it. As such, a poorly crafted model may generate incorrect insights or lead analysts to wrong conclusions.
 - The absence of a particular factor should not imply that it is not relevant to the issue at hand.
 - For the same particular problem, multiple teams may come up with competing models that appear very different. This does not mean that one is right and the others are wrong. Rather, all may equally valid, the difference being the nature of the expertise that went into creating them. For example, the four competing factor-based models were developed by different groups of students charged with understanding how an adversary might rate the attractiveness of different University assets.

E.1. DEVELOPING FACTOR-BASED MODELS STEPS

Step 1: Define and discuss the key risk question

Make sure the key risk question is clear and maximally unambiguous. Share the key risk question with others both involved and unininvolved with the issue and elicit their feedback.

For this step, also determine whether the desired factor-based model for the question at issue should be a value-type model (V-type) or a function-type model (F-type).

- A V-type model identifies dimensions of value and uses them to construct statements of higher order values (e.g., criticality and accessibility might relate to attractiveness).
- An F-type model identifies variables thought to influence an output via some sort of functional relationship (though such a relationship might not be defined in this model).

Knowing what type of model you are looking to create will also suggest what you can and cannot do with it.

Step 2: Articulate baseline assumptions

Use feedback received or any other motivations to explain what is precisely meant by the question to develop explanatory notes for the question. Such notes might crisply define the terminology used in the question, describe baseline assumptions underlying the question, clarify the context that the question applies to, and so on.

It is important to be as precise and accurate as possible to help future users of your model understand in what contexts it may be appropriate or inappropriate for use.

Step 3: Identify all relevant factors

It is often helpful to use brainstorming techniques, in particular Divergent-Convergent Thinking or Reverse Brainstorming, to assist in developing the list of factors.

For each factor, also provide guidance on how to make statements about the values or states it can take on. For example, if the factor is “vulnerability,” provide the user with insight into what is meant by “high

vulnerability” versus “low vulnerability,” and whether or not there is meaning in the way such statements are ordered (e.g., is “high vulnerability” better or worse than “low vulnerability”?).

Once the factors have been identified, this step requires you to clearly define each one in a manner similar to what was done for the key risk question in Step 2.

Step 4: Suggest how factors interact

Given the set of factors developed in Step 3, this step seeks to understand and describe the manner in which the factors interact in the model to produce an outcome or output. For example, you might say that “increased population” increases the potential “effects of an attack” due to a larger number of people that could be exposed to the circumstances surrounding the attack.

Step 5: Describe model limitations

Finally, after the model was constructed and described in terms of how it works, document the limitations and weaknesses associated with the model, or rather describe how the model might not work. This includes under what circumstances the model and its assumptions might not be valid, alternative points of view, and so on.

Follow-On Steps

It is often tempting to establish some quantitative-looking scoring scheme to each factor in a factor-based model which is then used in conjunction with some arithmetic function to produce numeric outputs. For example, the CARVER²⁹ methodology is often supplemented with a means to score each of the six model parameters accompanied by the suggestion that the sum of these scores provides a meaningful indication of overall target attractiveness.

As a word of caution, the addition of factors is typically not appropriate for F-type models (unless supported by data and appropriate analysis), and may not be appropriate for V-type models, particularly if the factors are not distinctly independent from one another. Moreover, many scoring schemes have severe limitations and built-in assumptions that may not be appropriate. However, the skeptical analyst might find the use of scoring and arbitrary math helpful in identifying the real relationships among variables by explaining why some alternative relationship is not appropriate. For example, one might discover that multiplication is appropriate in some instances by arguing why addition is inappropriate.

In general, resist the temptation to score and manipulate unless it is absolutely necessary. If scoring is viewed as being helpful and one can establish a reasonable ordering among the scores, opt to use the Sorting structured analytic technique ([Appendix V](#)) instead as it often generates the same if not better insights than what might be obtained using some mathematical operation.

²⁹ CARVER is a factor-based model developed by the U.S. Special Forces community in the early 1960s to quickly assess a number of targets and select the most appropriate target for the given mission. Since around the mid-1990s, this methodology has also been used by security practitioners to identify what an adversary might look to attack within their systems.

This page is intentionally blank.

APPENDIX F. EVENT MAPPING

What is it? Organizing the who, what, where, when, why, and how of an event is the goal of this graphic organizer. It produces a mind-mapping diagram representing the scenarios in hypotheses linked around a central word or short phrase representing the issue or problem to be analyzed.³⁰

Why use it?

Helps generate new ideas. The image-centered diagram with connections between events in a scenario on a radial encourages a brainstorming approach to the Event Mapping. The large amount of association in event maps promotes creativity in generating new ideas and associations not previously considered. The elements are arranged intuitively according to the importance of the concepts and are organized into groupings, branches, or areas.

Helps recall memories. The uniform graphic formulation of the semantic structure of information on the method of gathering knowledge may aid recall of existing memories.

Mitigation of bias. As scenario event hypotheses are mapped radially around the issue or problem without the implied prioritization that comes from hierarchy or sequential arrangements, anchoring and other cognitive bias can be mitigated to some degree.

Timing Assess Phase: Use this technique when a nonlinear method is desired to generate, visualize, structure, and delineate the events in a scenario or hypotheses related to the intelligence issue or problem. The addition of colors can represent key players in each scenario, such as economics, military, opposition group, science, culture, as well as internal and external political pressures. It is also easy to annotate indicators of change to use in the formation of collection plans.

Steps Event Mapping consists of the following eight steps:

Step 1: Put the word or symbol representing the issue or problem to be analyzed in the center of the paper or white board. Take a minute to think about it before continuing.

Step 2: Add symbols or words to represent hypotheses around the central issue or problem.

Step 3: Link the hypotheses to the central issue or problem. Use color to indicate the major influence the link represents. For example, use green for economic links, red for opposition groups, purple for military forces, blue for recognized legal political movements, black for external pressures, brown for cultural based links, etc.

³⁰ A Tradecraft Primer: Basic Structured Analytic Techniques. Defense Intelligence Agency. March 2008, pp. 55-57.

Step 4: Continue working outward, building the scenario of events into branches and sub-branches for each hypothesis in greater detail.

Step 5: Use emphasis, such as underlining and stars, to show importance or level of influence.

Step 6: Do not allow yourself or the group to get stuck in one scenario. If you dry up, move to another area or another hypothesis.

Step 7: When the creativity dies down, stop and take a break. After a period of an hour or so, return and review the map, making additions and changes as desired.

Step 8: As an option, you can add a number on links or decision points in each hypothesis and, on a separate piece of paper, write down the evidence for each number to be collected that would disprove that link or decision being made. Use the lists for each number to develop an integrated collection strategy for the issue or problem.

Tips**The general rules of Event Mapping are:**

- Start with a blank paper or use Post-it notes on a white board.
- Think in terms of key words, phrases, or symbols that represent ideas and words.
- Put down ideas as they occur, wherever they fit.
- Do not judge or hold back.
- Develop in directions the topic takes you — not limited by how you are doing the map.
- Become more detailed as you expand the map.
- Use arrows or other visual aids to show the links between events in the scenario.

Think fast. Your brain works best in 5- to 7-minute bursts, so capture that explosion of ideas as rapidly as possible.

Keep moving. If ideas slow down, draw empty lines, and watch your brain automatically find ideas to put on them. Stand up and use an easel pad or white board to generate even more energy.

Include distractions. If you are mapping and you suddenly remember you need to pick up your cleaning, put down “cleaning” on the side of the map. Otherwise your mind will get stuck like a record in that “cleaning” groove.

Write on links. Put key words on lines to give context to the link.

Print words. Print rather than write in script. It is easier to read and remember. Lowercase is more visually distinctive (and easier to remember) than uppercase.

Loss of Focus. Unconstrained Event Mapping can become overly detailed, lose focus, and include events and scenarios that lack relevance to the issue or problem being studied.

This page is intentionally blank.

APPENDIX G. EVENT TREE ANALYSIS

What is it? An Event Tree is a visual depiction of the downstream events resulting from the occurrence of an initiating event affecting a system. An Event Tree represents the various accidents or response scenarios that can occur following a particular event. Toward that end, an Event Tree starts with an initiating event and develops scenarios based on whether a system succeeds or fails in performing its functions. The Event Tree then considers all of the related systems that could respond to an initiating event, until the sequence ends in one of among multiple outcome states.³¹

Why use it? An Event Tree is a visual tool by which analysts can depict an adversary's options with decision points that gives insight into potential vulnerabilities. It clarifies the presumed sequence of causal or temporal events or decisions between an initiating event and a final outcome. Event Trees also provide an excellent method of determining collection requirements for the indications that a decision has been made or events have unfolded in one of the alternative limbs of the tree.³²

- End events need not be foreseen.
- Multiple failures can be analyzed.
- Potential single-point failures can be analyzed.
- System weaknesses can be identified.
- Zero-payoff system elements/options can be disregarded.
- Visualize event chains following the occurrence of an initiating event.
- Visualize barriers and sequence of activation.
- Good basis for evaluating the need for new / improved procedures and safety functions.

Timing Assess Phase: Use an Event Tree to clarify alternative event sequences leading to different future outcomes. Event Trees work best when there are multiple, mutually exclusive options that cover the spectrum of reasonable alternatives available.

³¹ "Event Tree." NRC. 27 May 2011. <<http://www.nrc.gov/reading-rm/basic-ref/glossary/event-tree.html>>.

³² *A Tradecraft Primer: Basic Structured Analytic Techniques*. Defense Intelligence Agency. 2008, pp. 51-54.

Steps The method for constructing and evaluating an Event Tree is comprised of the following eight steps. Construction of an Event Tree presumes that a desired “objective outcome” set is defined, for example {death, no death}, {no damage, partial damage, total damage}, etc.

1. Identify an initiating event that may give rise to unwanted consequences.
2. Identify circumstances that might exaggerate or alleviate the intensity of this initiating event.
3. Identify the barriers, countermeasures, mitigation strategies or interventions that are designed to deal with the event.
4. Construct the Event Tree depicting the sequence of events between cause and consequence.
5. Identify all potential scenarios and describe the outcomes.
6. Assign conditional probabilities to the branches and calculate the probability of each scenario.
7. Tally the probabilities for each unique outcome.
8. Compile and present the results from the analysis.

Tips An analytic failure can occur when the adversary selects an unforeseen option arising from ignorance or when an unidentified event occurs.

- Operating pathways must be anticipated.
- Partial successes/failures are not distinguishable.
- Initiating events are treated singly (multiple trees are required for multiple events).
- Sequence-dependent scenarios are not modeled well.
- No standard for graphical representation.
- Only one initiating event can be studied in a single Event Tree.
- Easy to overlook subtle system dependencies.

G.1. EVENT TREE ANALYSIS

Step 1: Identify an initiating event that may give rise to unwanted consequences. Identify the mutually exclusive (not overlapping) and collectively exhaustive (complete) set of hypotheses that pertain to a given risk issue.

Step 2: Decide which events, factors, or decisions (i.e., variables) will have the greatest influence on the alternatives or hypotheses identified in Step One. Each event should be presented as a negative statement.

Step 3: Decide on the temporal or causal order (sequence) in which these factors are expected to occur or impact one another. Each event should be presented as a negative statement. Cause-consequence; consequence becomes the cause of a subsequent event.

Step 4: Determine the event options within each alternative (hypothesis) and establish clear definitions for each event option to ensure collection strategies to monitor events are effective.

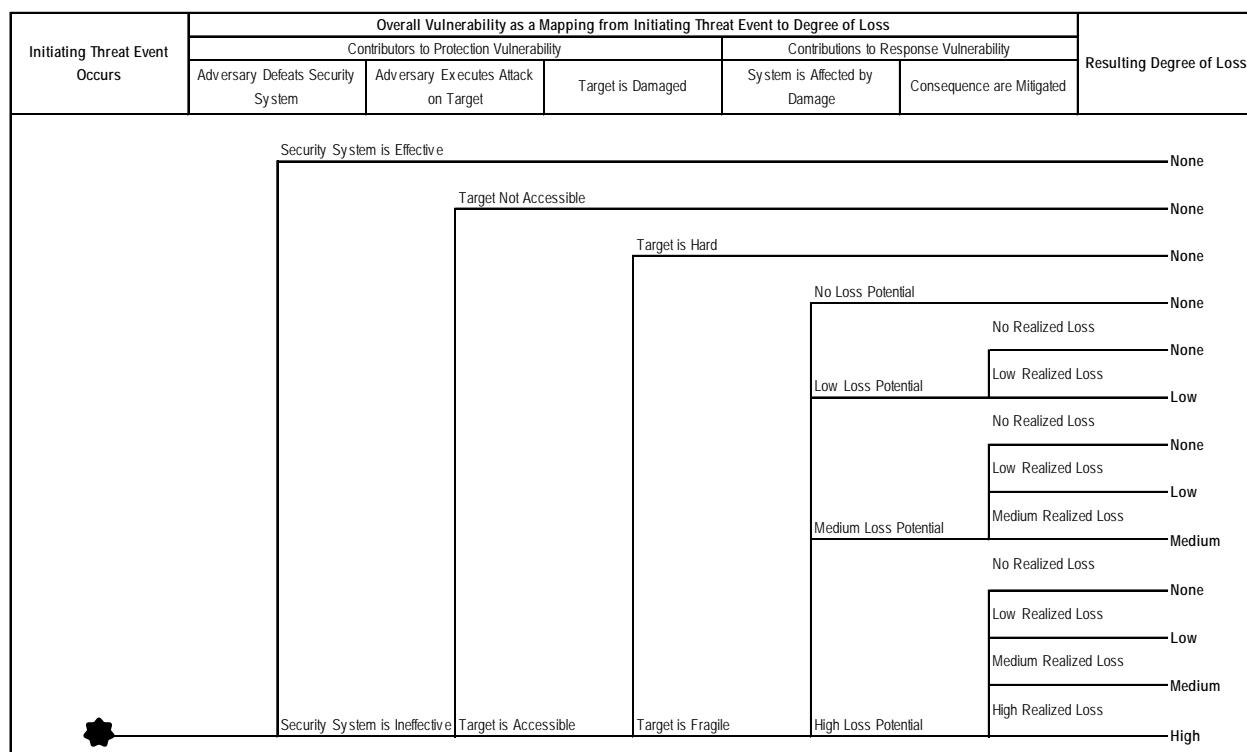
Step 5: Construct the Event Tree depicting the sequence of events between cause and consequence. Construct the Event Tree from left to right. Each alternative or hypothesis is a separate main branch. Start with the first alternative and have one branch from this node for each realistic path the first event can take. For instance, the purchased equipment could be used for its intended purpose, or it could be reverse-engineered for duplication, or it could be disassembled and sold for scrap. Proceed down each event option node until the end state for that sub-branch is reached. Then move to the next alternative or hypothesis and repeat the process.

Step 6: Determine what would indicate a decision has been made at each decision point, for each option, to use in generating an integrated collection plan.

Step 7: Assess the implications or aftereffects of each alternative on the key risk problem.

G.2. ILLUSTRATIVE EXAMPLE

The following example illustrates an Event Tree constructed for a security system.³³



³³ Shul'man, G. S. "Evaluating the Reliability of Nuclear Power Plant Protective Structures to an Airplane Crash." *Atomic Energy*, Vol. 81, No. 6. 1996, pp. 890-893. Print.

This page is intentionally blank.

APPENDIX H. EXPERT-OPIINION ELICITATION PROCESS

What is it? Expert-opinion elicitation is defined as a formal, heuristic process of obtaining information or answers to specific questions about certain quantities, called issues, such as failure rates, probabilities of events, failure consequences and expected service lives. The suggested steps for an expert-opinion elicitation process depend on the use of a technical integrator (TI) or a technical integrator and facilitator (TIF). The details of the steps involved in these two processes are defined in subsequent subsections. The technical integrator and facilitator is commonly used in practice and is utilized in this study.

The Expert-Opinion Elicitation Process was contributed by Bilal M. Ayyub, University of Maryland, College Park based on his 2001 text, *Elicitation of Expert Opinions for Uncertainty and Risks*.³⁴

Why use it? The value of the expert-opinion elicitation comes from its initial intended uses as a heuristic tool, not a scientific tool, for exploring vague and unknown issues that are otherwise inaccessible.

Timing All Phases: The primary reason for using expert-opinion elicitation is to deal with uncertainty in selected technical issues related to a system of interest. Issues with significant uncertainty, issues that are controversial and/or contentious, issues that are complex, and/or issues that can have a significant effect on risk are most suited for expert-opinion elicitation.

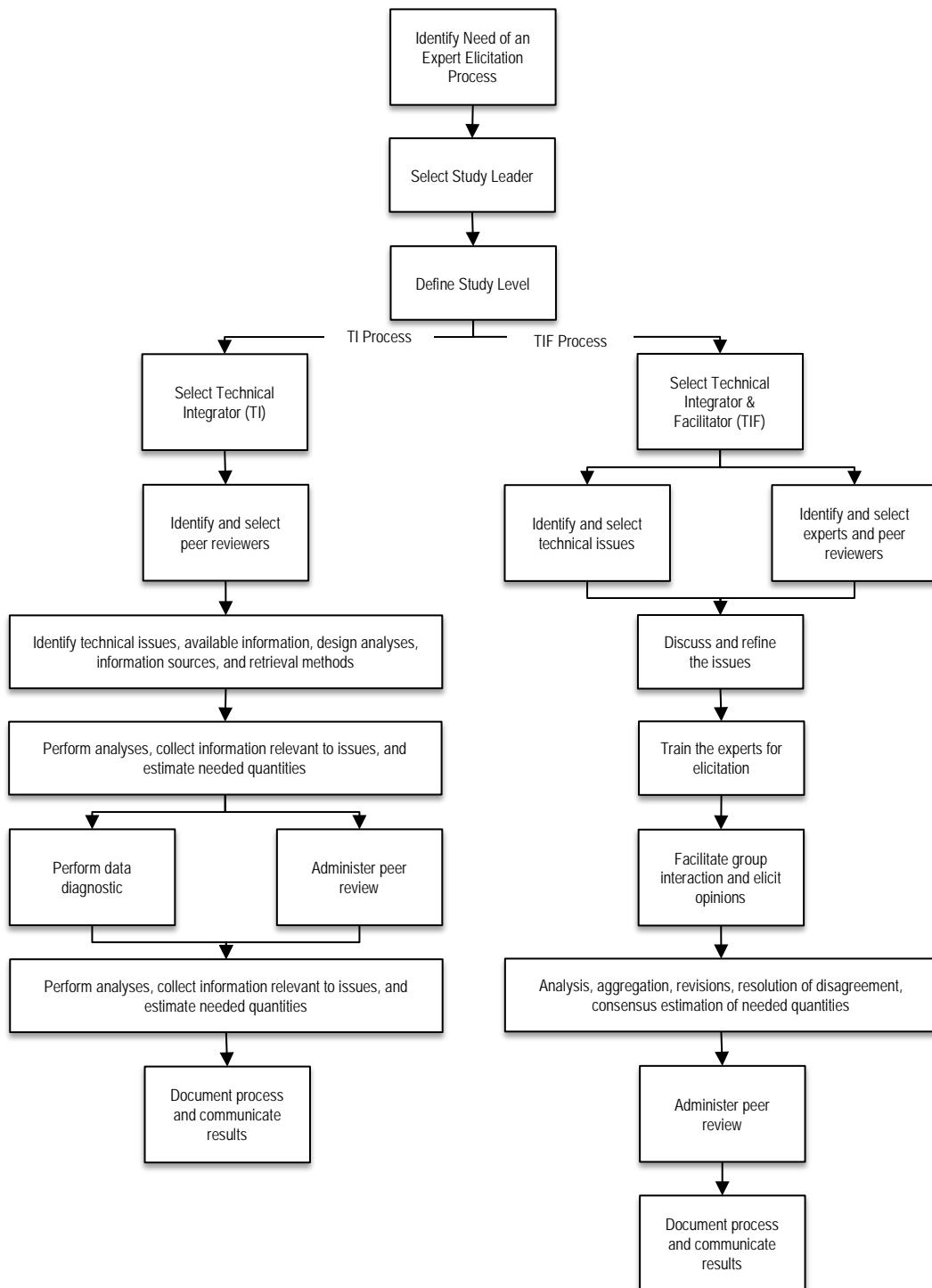
Steps The expert opinion elicitation process consists of the following nine steps:

1. Need identification
2. Select study level and study leader
3. Identify and select peer reviewers
4. Identify and select experts
5. Identify and select observers (optional)
6. Prepare read-ahead materials to experts and peer-reviewers
7. Identification, selection, and development of technical issues
8. Elicitation of opinions
9. Documentation and communication

Tips Expert opinion elicitation is not a substitute to scientific, rigorous research.

³⁴ Ayyub, Bilal M. *Elicitation of Expert Opinions for Uncertainty and Risks*. Boca Raton: CRC, 2001. Print.

H.1. SUBJECT-MATTER EXPERT SELECTION OVERVIEW



H.2. SUBJECT-MATTER EXPERT SELECTION STEPS

Step 1: Need identification

The identification of need and its communication to experts are essential for the success of the expert opinion elicitation process. The need identification and communication should include the definition of the goal of the study and relevance of issues to this goal. Establishing this relevance would make the experts stakeholders and thereby increase their attention and sincerity levels. Relevance of each issue and/or question to the study needs to be established. This question-to-study relevance is essential to enhancing the reliability of collected data from the experts. Each question or issue needs to be relevant to each expert especially when dealing with subjects with diverse views and backgrounds.

Step 2: Select study level and study leader

The goal of a study and nature of issues determine the study level. The study leader can be a technical integrator (TI), technical facilitator (TF), or a combined technical integrator and facilitator (TIF). The leader of the study is an entity having managerial and technical responsibility for organizing and executing the project, overseeing all participants, and intellectually owning the results. Expert-opinion elicitation commonly utilizes a TI or TIF leader. The primary difference between the TI and the TIF is in the intellectual responsibility for the study where it lies with only the TI, and the TIF and the experts, respectively. The TIF has also the added responsibility of maintaining the professional integrity of the process and its implementation. The TI is required to utilize peer reviewers for quality assurance purposes. A study leader should be selected based on the following attributes:

- An outstanding professional reputation, and wide recognition and competence based on academic training and relevant experience;
- Strong communication skills, interpersonal skills, flexibility, impartiality, and ability to generalize and simplify;
- A large contact base of industry leaders, researcher, engineers, scientists, and decision makers; and
- An ability to build consensus, and leadership qualities.

The study leader does not need to be a subject expert, but should be knowledgeable of the subject-matter.

Step 3: Identify and select peer reviewers

Peer review can be classified according to peer-review method, and according to peer-review subject. Two methods of peer review can be performed: 1) participatory peer review that would be conducted as an ongoing review throughout all study stages, and 2) late-stage peer review that would be performed as the final stage of the study. The second classification of peer reviews is by peer-review subject and has two types: 1) technical peer review that focuses on the technical scope, coverage, contents and results, and 2) process peer review that focuses on the structure, format and execution of the expert-opinion elicitation process.

Peer reviewers are needed for both the TI and TIF processes. The peer reviewers should be selected by the study leader in close consultation with perhaps the study sponsor. The following individuals should be sought after in peer reviewers:

- Researchers, scientists, and/or engineers that have outstanding professional reputation, and widely recognized competence based on academic training and relevant experience.
- Researchers, scientists, and/or engineers with general understanding of the issues in other related areas, and/or with relevant expertise and experiences from other areas.
- Researchers, scientists, and/or engineers who are available and willing to devote the needed time and effort.
- Researchers, scientists, and/or engineers with strong communication skills, interpersonal skills, flexibility, impartiality, and ability to generalize and simplify.

Step 4: Identify and select experts

The size of an expert panel should be determined on a case-by-case basis. The size should be large enough to achieve a needed diversity of opinion, credibility, and result reliability. In recent expert-opinion elicitation studies, a nomination process was used to establish a list of candidate experts by consulting archival literature, technical societies, governmental organizations, and other knowledgeable experts. Formal nomination and selection processes should establish appropriate criteria for nomination, selection, and removal of experts. For example, the following criteria was used in a Yucca Mountain seismic hazard analysis to select experts:

- Strong relevant expertise through academic training, professional accomplishment and experiences, and peer-reviewed publications;
- Familiarity and knowledge of various aspects related to the issues of interest;
- Willingness to act as proponents or impartial evaluators;
- Availability and willingness to commit needed time and effort;
- Specific related knowledge and expertise of the issues of interest;
- Willingness to effectively participate in needed debates, to prepare for discussions, and provide needed evaluations and interpretations; and
- Strong communication skills, interpersonal skills, flexibility, impartiality, and ability to generalize and simplify.

In some studies, criteria was set for expert removal that included failure to perform according to commitments and demands as set in the selection criteria and unwillingness to interact with members of the study.

The panel of experts for an expert-opinion elicitation process should have a balance and broad spectrum of viewpoints, expertise, technical points of view, and organizational representation. The diversity and completeness of the panel of experts is essential for the success of the elicitation process. For example, it should include the following groups:

- Proponents who advocate a particular hypothesis or technical position.
- Evaluators who consider available data, become familiar with the views of proponents and other evaluators, questions the technical bases of data, and challenges the views of proponents.
- Resource experts who are technical experts with detailed and deep knowledge of particular data, issue aspects, particular methodologies, or use of evaluators.

The experts should be familiar with the design, operation, performance, etc. of the system or issue of interest. It is essential to select people with basic domain-specific technological knowledge; however, they do not necessarily need to be all engineers and/or economists or PhD-level scientists. It might be necessary to include one or two experts from management with engineering knowledge of the equipment and components, consequences, safety aspects, administrative and logistic aspects of operation, expert-opinion elicitation process, and objectives of this study. One or two experts with a broader knowledge of the equipment and components might be needed. Also, one or two experts with a background in risk analysis and risk-based decision making and their uses in areas related to the facility of interest might be needed.

Step 5: Identify and select observers (optional)

Observers can be invited to participate in the elicitation process. Observers can contribute to the discussion, but cannot provide expert opinions that enter into the aggregated opinion of the experts. The observers provide expertise in the elicitation process, probabilistic and statistical analyses, risk analysis, and other support areas. The composition and contribution of the observers are essential for the success of this process. The observers may include the following:

- Individuals with research or administrative-related background from research laboratories or the U.S. Army Corps of Engineers with engineering knowledge of equipment and components of Corps facilities.
- Individuals with expertise in probabilistic analysis, probabilistic computations, consequence computations and assessment, and expert-opinion elicitation.

A list of names with biographical statements of the study leader, technical integrator, technical facilitator, experts, observers, and peer reviewers should be developed and documented. All attendees can participate in the discussions during the meeting. However, only the experts can provide the needed answers to questions on the selected issues. The integrators and facilitators are responsible for conducting the expert-opinion elicitation process. They can be considered a part of the observers or experts depending on the circumstances and the needs of the process.

Step 6: Prepare read-ahead materials to experts and peer-reviewers

The experts and observers need to receive the following items before the expert-opinion elicitation meeting:

- An objective statement of the study.
- A list of experts, observers, integrators, facilitators, study leader, sponsors, and their biographical statements.
- A description of the facility, systems, equipment, and components.
- Basic terminology, definitions that should include probability, failure rate, average time between failures, mean (or average) value, median value, and uncertainty.
- Failure consequence types.
- A description of the expert-opinion elicitation process.
- A related example on the expert-opinion elicitation process and its results, if available.
- Aggregation methods of expert opinions such as computations of percentiles.
- A description of the issues in the form of a list of questions with background descriptions.

- Each issue should be presented on a separate page with spaces for recording an expert's judgment, any revisions, and comments.
- Clear statements of expectations from the experts in terms of time, effort, responses, communication, and discussion style and format.

It might be necessary to personally contact individual experts for the purpose of establishing clear understanding of expectations.

Step 7: Identification, selection, and development of technical issues

The technical issues of interest should be carefully selected to achieve certain objectives. In these guidelines, the technical issues can be related to the quantitative assessment of failure probabilities and consequences for selected components, subsystems, and systems within a facility. The issues should be selected such that they would have a significant impact on the study results. These issues should be structured in a logical sequence starting by background statement, followed by questions, and then answer selections or answer format and scales. Personnel with a risk-analysis background and familiar with the construction, design, operation, and maintenance of the facility need to define these issues in the form of specific questions. Also, background materials about these issues need to be assembled. The materials will be used to familiarize and train the experts about the issues of interest as described in subsequent steps.

An introductory statement for the expert-opinion elicitation process should be developed that includes the goal of the study and establishes relevance. Instructions should be provided with guidance on expectations, answering the questions, and reporting. The following are guidelines on constructing questions and issues based social research practices:

- Each issue can include several questions, however, each question should consist of only one sought after answer. It is a poor practice to include two questions in one.
- Question and issue statements should not be ambiguous. Also, the use of ambiguous words should be avoided. In expert-opinion elicitation of failure probabilities, the word "failure" might be vague or ambiguous to some subjects. Special attention should be given to its definition within the context of each issue or question. The level of wording should be kept to a minimum. Also, the choice of the words might affect the connotation of an issue especially by different subjects.
- The use of factual questions is preferred over abstract questions. Questions that refer to concrete and specific matters result in desirable concrete and specific answers.
- Questions should be carefully structured in order to reduce biases of subjects. Questions should be asked in a neutral format, sometimes more appropriately without lead statements.
- Sensitive topics might require stating questions with lead statements that would establish supposedly accepted social norms in order to encourage subjects to answers the questions truthfully.

Questions can be classified into open-ended questions and closed-ended questions. The format of the question should be selected carefully. The format, scale and units for the response categories should be selected to best achieve the goal of the study. The minimum number of questions and question order should be selected using practices and methods of educational and psychological testing and social research.³⁵

³⁵ Ayyub, Bilal M. *Elicitation of Expert Opinions for Uncertainty and Risks*. Boca Raton: CRC, 2001. Print.

Once the issues are developed, they should be pretested by administering them to a few subjects for the purpose of identifying and correcting flaws. The results of this pretesting should be used to revise the issues.

Step 8: Elicitation of opinions

The elicitation process of opinions should be systematic for all the issues according to the steps presented in this section.

Part One (8-1): Issue familiarization of experts. The background materials that were assembled in the previous step should be sent to the experts about one to two weeks in advance of the meeting with the objective of providing sufficient time for them to become familiar with the issues. The objective of this step is, also, to ensure that there is a common understanding among the experts of the issues. The background material should include the objectives of the study, description of the issues and lists of questions for the issues, description of systems and processes, their equipment and components, the elicitation process, selection methods of experts, and biographical information on the selected experts. Also, example results and their meaning, methods of analysis of the results, and lessons learned from previous elicitation processes should be made available to them. It is important to breakdown the questions or issues in components that can be easily addressed. Preliminary discussion meetings or telephone conversations between the facilitator and experts might be necessary in some cases in preparation for the elicitation process.

Part Two (8-2): Training of experts. This step is performed during the meeting of the experts, observers and facilitators. During the training the facilitator needs to maintain flexibility to refine wording or even change approach based on feedback from experts. For instance, experts may not be comfortable with “probability” but they may answer on “events per year” or “recurrence interval.” The meeting should be started with presentations of background materials to establish relevance of the study to the experts, and study goals in order to establish rapport with the experts. Then, information on uncertainty sources and types, occurrence probabilities and consequences, expert-opinion elicitation process, technical issues and questions, aggregation of expert opinions should be presented. Also, experts need to be trained on providing answers in an acceptable format that can be used in the analytical evaluation of the failure probabilities or consequences. The experts need to be trained in certain areas such as the meaning of probability, central tendency, and dispersion measures especially to experts who are not familiar with the language of probability. Additional training might be needed on consequences, subjective assessment, logic trees, problem structuring tools such as Influence Diagrams, and methods of combining expert evaluations. Sources of bias that include overconfidence, and base-rate fallacy and their contribution to bias and error should be discussed. This step should include a search for any motivational bias of experts due to, for example, previous positions experts have taken in public, wanting to influence decisions and funding allocations, preconceived notions that they will be evaluated by their superiors as a result of their answers, and/or to be perceived as an authoritative expert. These motivational biases, once identified, can be sometimes overcome by redefining the incentive structure for the experts.

Part Three (8-3): Elicitation and collection of opinions. The opinion elicitation step starts with a technical presentation of an issue, and by decomposing the issue to its components, discussing potential influences, and describing event sequences that might lead to top events of interest. These top events are the basis for questions related to the issue in the next stage of the opinion elicitation step. Factors, limitations, test results, analytical models, and uncertainty types and sources need to be presented. The presentation should allow for questions to eliminate any ambiguity and clarify scope and conditions for

the issue. The discussion of the issue should be encouraged. The discussion and questions might result in refining the definition of the issue. Then, a form with a statement of the issue should be given to the expert to record their evaluation or input. The experts' judgment along with their supportive reasoning should be documented about the issue. It is common that experts would be asked to provide several conditional probabilities in order to reduce the complexity of the questions and thereby obtain reliable answers. These conditional probabilities can be based on fault tree and Event Tree diagrams.

Conditioning has the benefit of simplifying the questions by decomposing the problems. Also, it results in a conditional event that has a larger occurrence probability than its underlying events; therefore making the elicitation less prone to biases since experts tend to have a better handle on larger probabilities in comparison to very small ones. It is desirable to have the elicited probabilities in the range of 0.1 to 0.9 if possible. Sometimes it might be desirable to elicit conditional probabilities using linguistic terms as described by Ayyub.³⁶ If correlation among variables exists, it should be presented to the experts in great detail and conditional probabilities need to be elicited.

Issues should be dealt with one issue at a time, although sometimes similar or related issues might be considered simultaneously.

Part Four (8-4): Aggregation of results. The collected assessments from the experts for an issue should be assessed for internal consistency, analyzed and aggregated to obtain composite judgments for the issue. The means, medians, percentile values and standard deviations need to be computed for the issues. Also, a summary of the reasoning provided during the meeting about the issues needs to be developed.

Uncertainty levels in the assessments should also be quantified. A summary of methods for combining expert opinions was provided by Ayyub.³⁷ The methods can be classified into consensus methods and mathematical methods. The mathematical methods can be based on assigning equal weights to the experts or different weights.

Part Five (8-5): Group interaction, discussion, and revision by experts. The aggregated results need to be presented to the experts for a second round of discussion and revision. The experts should be given the opportunity to revise their assessments of the individual issues at the end of the discussion. Also, the experts should be asked to state the rationale for their statements and revisions. The revised assessments of the experts need to be collected for aggregation and analysis. This step can produce either consensus or no consensus. The selected aggregation procedure might require eliciting weight factors from the experts. In this step the technical facilitator plays a major role in developing a consensus, and maintaining the integrity and credibility of the elicitation process. Also, the technical integrator is needed to aggregate the results without biases with reliability measures. The integrator might need to deal with varying expertise levels for the experts, outliers (i.e., extreme views), non-independent experts, and expert biases.

Step 9: Documentation and communication

A comprehensive documentation of the process is essential in order to ensure acceptance and credibility of the results. The document should include complete descriptions of the steps, the initial results, revised results, consensus results, and aggregated results spreads and reliability measures.

³⁶ Ayyub, Bilal M. *Elicitation of Expert Opinions for Uncertainty and Risks*. Boca Raton: CRC, 2001. Print.

³⁷ Ayyub, Bilal M. *Elicitation of Expert Opinions for Uncertainty and Risks*. Boca Raton: CRC, 2001. Print.

This page is intentionally blank.

APPENDIX I. FAILURE MODES AND EFFECTS ANALYSIS

What is it? Failure Modes and Effects Analysis (FMEA) is a formal systematic approach to identifying how a system could fail, the causes of such failure, and the effects of its occurrence on the system operation. FMEA is a bottom-up approach for identifying potential system failures and unacceptable failure effects. FMEA is used in many system design analyses including assessing system safety, planning maintenance activities, identifying developing countermeasures and mitigation options.³⁸ The definitions of the key words in the name FMEA are as follows:

- Failure modes are the ways in which a system might fail. A failure is any error or defect in a part of the system that could impact its functioning and performance. Failures can be potential (latent) or active.
- Effects are the consequences on the system due to the occurrence of a failure mode. Effects are also referred to as outcomes.

In a FMEA, failure modes are prioritized or rank ordered according to how serious their consequences are on the system, how frequently they occur and how easily they can be detected. The purpose of the FMEA is to take actions to eliminate or reduce failures starting with the actions of highest-priority.

FMEA originated as a military procedure that dates back to the 1949 issue of MIL-P-1629 that described a process to assess the impact a particular failure would have on the success of an associated mission or on the health and safety of personnel and equipment. Over the following decade FMEA grew in popularity throughout the military industrial complex. In the mid-1960s, NASA adopted FMEA to analyze safety issues during the Apollo Program. Shortly after its use by NASA FMEA became a key tool for improving safety in general across all many industries, especially in the chemical process industries. The goal with safety FMEAs was, and remains today to prevent safety accidents and incidents from occurring.³⁹ For example, in the 1970's the Ford Motor Company began to apply FMEA as a quality improvement tool after safety issues that arose with their Pinto line.⁴⁰ Today, detailed procedures for FMEA are available in a number of textbooks on reliability engineering. The military codified one approach to FMEA and its cousin FMECA in MIL-STD-1629A in 1980.⁴¹ However, as of 4 August 1998, this standard was cancelled; users were urged to consult various national and international documents for information regarding FMEA/FMECA.

³⁸ "Failure Modes and Effects Analysis (FMEA)." ASQ: The Global Voice of Quality. n.d. Web. <<http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html>>.

³⁹ McDermott, Robin E., Raymond J. Mikulak, and Michael R. Beauregard. *The Basics of FMEA*. New York: Quality Resources, 1996. Print.

⁴⁰ Herman, Rich. "Failure Mode and Effects Analysis (FMEA) Basics." Ezine Articles. 6 January 2007. <<http://ezinearticles.com/?Failure-Mode-and-Effects-Analysis-%28FMEA%29-Basics&id=406935>>.

⁴¹ *Procedures for Performing Failure Modes, Effects and Criticality Analysis*. U.S. Department of Defense. 24 November 1980. <<http://src.alionscience.com/pdf/MIL-STD-1629RevA.pdf>>.

Why use it?

Disciplined analysis - FMEA is a structured process that promotes the disciplined elicitation of ideas about the kinds of failures that may occur in a system, careful analysis of specific risk/hazard and vulnerability areas, proper documentation of sources and assumptions, and identification of interventions that manage risks to an acceptable level.⁴² Specifically, a FMEA systematically, comprehensively, and critically examines a system so as to provide answers to the following questions:

- How can components of the system fail?
- Under what circumstances would they fail?
- What is the likeliness that they would fail?
- How would a particular failure mode impact overall system performance?
- Would we receive adequate warning or signs of an imminent or emerging failure?
- How can failure be prevented?

Like most structured analysis methodologies, the FMEA methodology helps the analyst construct a risk/vulnerability-oriented representation of a system from scratch. Also, an FMEA product may be adopted by other analysts for use in enhancing their own representation of the system.

Clear documentation of analysis - FMEA provides a framework for documenting and tracking knowledge and actions about system threats, vulnerabilities, and consequences. In a sense, a FMEA table may be viewed as a type of risk register. FMEA captures the collective knowledge of a team with respect to a system of interest. Moreover, FMEA has been noted as a “catalyst for teamwork and idea exchange.”⁴³

Produces rank orderings of vulnerabilities based on risk - FMEA produces a rank-ordered risk of failure modes based on risk, where risk is assessed as the product of probability and consequence. However, while FMEA might reveal that one risk is ranked higher than another, it will not directly indicate the extent of this difference.

Synergistic with other structured analysis techniques - Use of FMEA is significantly enhanced if performed together with a top-down approach such as Fault Tree Analysis ([Appendix J](#)). Combined, FMEA as a bottom-up approach and Fault Tree Analysis as a top-down approach helps the analyst look at the system from all angles.

⁴² Berman, Benjamin A. “Effective Risk Management and Quality Improvement by Application of FMEA and Complementary Techniques.” ParagonRx. November 2003. <<http://www.paragonrx.com/experience/white-papers/effective-risk-management-and-quality-improvement/>>.

⁴³ “Failure Modes and Effects Analysis (FMEA).” New Product Development Solutions. 4 April 2007. Web. 2 June 2011. <<http://www.npd-solutions.com/fmea.html>>.

Timing

All Phases: FMEA can be used in any of the following situations familiar to the homeland security and emergency management communities:

- To identify, assess, and rank order vulnerabilities of a system (how it can fail or be made to fail).
- To assess the effect an exploited vulnerability could have on the system as a whole.
- To imagine potential causes of failure, whether accidental or intentional.
- To identify opportunities for mitigation and vulnerability reduction.
- To establish goals for improving the effectiveness of system performance (e.g., response times).
- To track and monitor system risks (see the article on Risk Register).

In many ways, a FMEA is similar in scope to a systems vulnerability and risk assessment. The following are example generic FMEA application areas:

- Process FMEA: analysis of a process, to include training, plan, procedure, etc.
- Mission FMEA: analysis of a mission profile (also Functional FMEA).
- Design FMEA: analysis of products or technology prior to production (technology evaluation).
- Concept FMEA: analysis of systems in the early design concept stages.
- Equipment FMEA: analysis of machinery and equipment design before purchase.
- Service FMEA: analysis of service industry processes before they are released to impact the customer.
- System FMEA: analysis of the global system functions.
- Software FMEA: analysis of the software functions.

A FMEA is typically viewed as a living analysis. FMEAs are typically performed on a continuous basis and maintained as part of a comprehensive quality program that seeks to identify and mitigate the potential for system failures.

Steps The overall approach for conducting an FMEA is comprised of the following six steps:

1. Analysis setup
2. Identify failure modes
3. Estimate effects of failure and their severity rating
4. Identify potential causes of failure and estimate their likeliness
5. Estimating detection and its effectiveness
6. Summary and follow-on analysis

Data to support an FMEA includes:

- Data on historical events
- Documentation on how the system works (e.g., process maps)
- Experienced judgment of individuals belonging to the system

Tips A number of structured analytic techniques may help with performing different activities and steps associated with an FMEA, including:

- Brainstorming Techniques
 - Delphi Method ([Appendix C.1](#))
 - Divergent-Convergent Thinking ([Appendix C.3](#))
 - CIA Approach to Divergent-Convergent Thinking ([Appendix C.3.a](#))
 - DIA Approach to Divergent-Convergent Thinking ([Appendix C.3.b](#))
 - Outside-In Thinking ([Appendix C.4](#))
 - Reverse Brainstorming ([Appendix C.6](#))
 - Round-Robin Brainstorming ([Appendix C.5](#))
 - Murder Board
- System Description Methodology ([Appendix W](#))
- Fault Tree Analysis ([Appendix J](#))
- Cause and Effect Diagrams ([Appendix C](#))

I.1. FAILURE MODES AND EFFECTS ANALYSIS STEPS

Step 1: Analysis Setup

Establish the justification and purpose for the analysis, define the system under study, and establish the scope of the FMEA.

Part One (1-1): Describe why an FMEA is needed. Before starting a FMEA, describe the reasons for conducting a FMEA; to include – the types and nature of the decisions it may or may not support. A FMEA should only be performed if the value in doing so is expected to outweigh its cost.

Note: FMEA is not intended to be an afterthought exercise to justify decisions that have already been made. Rather, FMEA is intended to help users better understand their system in terms of how it can fail under normal and abnormal circumstances.

Part Two (1-2): Establish the FMEA Analysis Team. At a minimum, the team should be comprised of a single individual that is familiar with the FMEA process (e.g., Methodologist) and has the ability to identify and reach out to people with the necessary expertise. If more people are available to support this analysis, the ideal FMEA team should consist of 5-7 individuals with complementary knowledge that when combined, cover at least 80% of the required expertise. An example team in the context of studying resilience might be composed of the following people:

- Risk methodologist or risk analyst
- Experienced firefighter or rescue services official
- Experienced law enforcement official
- Local emergency manager or delegate
- Senior member of a volunteer organization (e.g., Red Cross)
- Experienced official from the public works department
- Experienced official from the transportation department
- Long-time resident of the jurisdiction or region

Part Three (1-3): Define the system under study. The system definition describes:

- One or more system objectives
- The physical (hardware), virtual (software), human (personnel), and logical (process) elements comprising the system (e.g., what elements make up the system?)
- The relationships between system elements and overall system performance (how do these elements interact?).

A number of methodologies may help characterize the system, including:

- System Description Methodology ([Appendix W](#))
- Cyber Footprinting
- A variety of brainstorming techniques
- Hierarchical Holographic Modeling ([Appendix L](#))

One goal from this step should be to construct a functional block diagram that illustrates all relevant system elements and how they relate to one another.

Part Four (1-4): Define the scope of the FMEA. The scope of the analysis specifies:

- Definitions for system failure as it relates to system objectives identified in the previous step.
- The types of causes that will be considered, including accidental, random, deliberate, and malicious.
- The nature of the analysis, such as whether it will be purely descriptive or have quantitative elements.
- Resources available for conducting analysis in terms of time, people, data, time on-site, etc.
- Constraints on the analysis, to include access limitations, information security requirements, etc.
- Keywords that characterize the types of expertise needed to complete this analysis.

Part Five (1-5): Complete and file the FMEA pre-analysis worksheet and review it with the customer. The worksheet should clearly articulate the scope of the analysis, team composition, expertise that will be consulted, any constraints on available resources, a concise definition of the system under study, and, to the maximum extent possible, what is not covered in the analysis. Once complete, make sure to review the pre-analysis worksheet with the client or customer for his concurrence. You may append to this pre-analysis any worksheets completed for supporting analytical activities.

Step 2: Identify Failure Modes

This step identifies ways in which components or elements of the system under study might fail. The following structured brainstorming techniques may be helpful for completing this step:

- Divergent-Convergent Thinking ([Appendix C.3](#))
- Premortem Analysis ([Appendix P](#))

Part One (2-1): Identify the important functions of each system element. Consider the following questions:

- What is the purpose of this system element?
- What does the system need this element to do?
- How does performance of this element relate to system performance?
- Is this a single point failure?

It may be helpful to treat some system elements as subsystems comprised of many smaller elements, each with their own purpose.

Part Two (2-2): Identify all plausible ways failure could happen for each system element. These are potential failure modes. If necessary, go back and rewrite the function with more detail to be sure the failure modes show a loss of that function. It may be helpful to apply one or more brainstorming techniques to answer this step.

Step 3: Estimate Effects of Failure and their Severity Rating

This step estimates system-level effects corresponding to the occurrence of each failure mode.

Part One (3-1): Identify all the consequences of each failure mode identified in Part 2 of Step 2.

Consider the following questions that seek to understand what happens when failure occurs:

- Does this failure cause failure of the systems or other systems?
- Does this failure disrupt the performance of other system elements?
- Does this failure increase the load on other elements?
- Does this failure decrease the reliability or increase the vulnerability of the system?
- Does this failure make other system elements more or less critical?
- What does the decision maker experience because of this failure?

Answers to these questions are potential effects of failure.

Part Two (3-2): Estimate the seriousness of each effect. This is the severity level or rating, also known as SEV. Specifically, SEV answers the following question: *How severe of an impact would be the outcome, following the occurrence of a particular failure mode?*

SEV is typically rated on an ordinal scale from 1 to 10, where 1 is insignificant and 10 is catastrophic.

Alternative scales may be used, including quantitative scales (interval, ratio and logarithmic scales), ordinal scales, and scales based on utility measures. If a failure mode has more than one effect, write on the FMEA table only the highest severity rating for that failure mode. A sample table of severity levels is shown below:

Severity Levels			
<i>Tailor the labels and definitions to meet your specific needs.</i>			
Rating	Description	Rating	Description
10	Severely High	5	Low
9	Extremely High	4	Very Low
8	Very High	3	Minor
7	High	2	Very Minor
6	Moderate	1	None

Step 4: Identify Potential Causes of Failure and Estimate their Likeliness

This step seeks to identify the reasons why failure of system elements might occur.

Part One (4-1): Determine all potential root causes for each failure mode. Depending on the scope of the analysis described in Part 4 of Step 1, causes might include accidental, random, common-cause, dependent, deliberate and malicious failures. List all possible causes for each failure mode on the FMEA worksheet. Tools to help with this step include:

- Brainstorming Techniques
 - Delphi Method ([Appendix C.1](#))
 - Divergent-Convergent Thinking ([Appendix C.3](#))
 - CIA Approach to Divergent-Convergent Thinking ([Appendix C.3.a](#))
 - DIA Approach to Divergent-Convergent Thinking ([Appendix C.3.b](#))
 - Outside-In Thinking ([Appendix C.4](#))
 - Reverse Brainstorming ([Appendix C.6](#))
 - Round-Robin Brainstorming ([Appendix C.5](#))
 - Murder Board
- Premortem Analysis ([Appendix P](#))
- Root Cause Analysis ([Appendix S](#))
- Anticipatory Failure Determination ([Appendix A](#))

Part Two (4-2): Estimate the likeliness of occurrence for each root cause. This is the occurrence level or rating, also known as OCC. Specifically, OCC answers the following question: *What is the likeliness that the particular failure mode caused by the particular failure mechanism will occur?*

OCC is typically rated on an ordinal scale from 1 to 10, where 1 is extremely unlikely and 10 is inevitable or guaranteed. Values of 0 for Occurrence may also be included. Alternative scales may be used for Occurrence, including quantitative scales (interval, ratio and logarithmic scales), ordinal scales, and scales based on uncertainty measures (e.g., probability). A sample table of occurrence levels is shown below:

Occurrence Levels			
<i>Tailor the labels and definitions to meet your specific needs.</i>			
Rating	Description	Rating	Description
10	Very High	5	Moderate
9	High	4	Moderately Low
8	High	3	Low
7	High	2	Low
6	Moderately High	1	Remote

Tip: It often helps to define a timeframe for which to evaluate the occurrence likeliness for each postulated root cause.

Step 5: Estimating Detection and its Effectiveness

This step assesses whether there are mechanisms in place or reliable cues in the environment that would assist in providing warning prior to the occurrence of high-severity failure modes.

Part One (5-1): Identify current failure detection capabilities. These are the diagnostic or prognostic tests, procedures, or mechanisms that you now have in place to identify or predict the onset of failure. These controls might prevent the cause from happening, reduce the likelihood that it will happen, or detect failure after the cause has already happened, but before the customer is affected. For example, for a power plant operator concerned with maintaining power generation, the ability to detect the onset of a malicious act against a generator will help decrease the risk associated with that event.

Part Two (5-2): Estimate the ability to warn about the onset of failure. This is a detectability level or rating, also known as DET. Specifically, DET answers the following question: *What is the likeliness that the onset of failure will be detected in enough time to do something about it?*

The DET rating estimates how well the controls can detect either the cause or its failure mode after they have happened, but before the system is affected. Detectability is typically rated on an ordinal scale from 1 to 10, where 1 means the control is absolutely certain to detect a problem prior to failure and 10 means the control is certain not to detect the problem. Values of 0 for Detectability may also be included. Alternative scales may be used for Occurrence, including quantitative scales (interval, ratio and logarithmic scales), ordinal scales, and scales based on uncertainty measures (e.g., probability and possibility). A sample table of Detectability Levels is shown below:

Detectability (DET) Levels			
<i>Tailor the labels and definitions to meet your specific needs.</i>			
Rating	Description	Rating	Description
10	Absolute Uncertainty	5	Moderate
9	Very Remote	4	Moderately High
8	Remote	3	High
7	Very Low	2	Very High
6	Low	1	Almost Certain

Note: Unlike with SEV and OCC where higher scores correspond to higher levels of severity and occurrence (respectively), higher scores for DET corresponds to a weaker (lesser) ability to predict the onset of failure (see Directionality of Assessment Criteria).

Step 6: Summary and Follow-On Analysis

This step determines a rank order of failure modes and summarizes the analysis in the form of a FMEA table.

Part One (6-1): Calculate the risk priority number. The risk priority number is labeled RPN and results from the product $SEV \times OCC \times DET$. Also calculate Criticality by multiplying severity by occurrence, $SEV \times OCC$. These numbers provide guidance for ranking potential failures in the order they should be addressed. This step, however, is not required to be done in this manner, and may be substituted with simple Sorting ([Appendix V](#)), Weighted Ranking ([Appendix X](#)), or augmented using quantitative risk analysis methods.

Note: RPNs cannot and should not be used for benefit cost analysis. The only exception that can be made to this rule is when meaningful quantitative scales are used for each of S (i.e., value measures), O (i.e., probability measures) and D (i.e., probability measures). However, it is appropriate to use the RPNs as a means for generating insight that could help you form qualitative arguments in favor or in opposition to a follow-on action.

Part Two (6-2): Complete the baseline FMEA table. For most practical systems requiring an FMEA, it is common to generate a lot of paper. Be sure to organize the FMEA in a manner that lends itself to providing the needed information quickly. The FMEA template is available for use.

Part Three (6-3): Develop actions for consideration. Such actions include:

- Strategies to mitigate the likeliness of postulated root causes of failure
- Strategies to eliminate one or more failure modes
- Strategies to reduce the severity of a particular failure mode
- Strategies to improve warning against failure

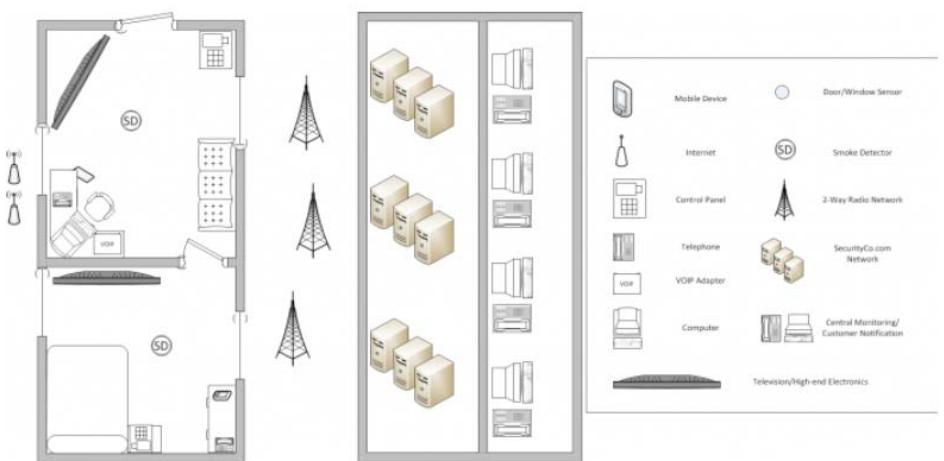
Insights obtained from FMEA often provides ample basis to support or challenge these decisions.

Part Four (6-4): Is this failure mode associated with a critical characteristic? (Critical characteristics are measurements or indicators that reflect safety or compliance with government regulations and need special controls.) If so, a column labeled “Classification” receives a Y or N to show whether special controls are needed. Usually, critical characteristics have a severity of 9 or 10 and occurrence and detection ratings above 3.

Part Five (6-5): Periodically revisit and revise the FMEA as changes are made. Remember, FMEA is a living analysis, and as such every so often the analysis should be looked at again to identify any changes in the system or operational environment.

I.2. ILLUSTRATIVE EXAMPLE

The following example considers a Home Security System that is packaged by a generic security company SecurityCo.com. The figure shown below represents all of the system’s working parts.



Step 1: Analysis Setup

Part One (1-1): Describe why an FMEA is needed. The owner of the home under analysis has recently purchased new kitchen appliances, furniture, and new high end consumer electronics (television, stereo system, and personal computer). These updates have significantly increased the value of the home along with an increased risk of a theft occurring. The home is located in an unsafe area and to reduce the uncertainty of a break-in the owner has decided to conduct a Failure Modes and Effects analysis on the security system to identify any areas of weakness.

Part Two (1-2): Establish the FMEA Analysis Team. The analysis of a home security system is a smaller scale project; therefore, it will only require one FMEA specialist to perform the analysis. The homeowner has chosen a Risk Analyst from a local University to perform the assessment of their system.

Part Three (1-3): Define the system under study. The security system being analyzed is a packaged security product provided by the commercial home security system provider SecurityCo.com. To properly define the system, it is important to identify the following:

1. System objectives
2. System elements
3. System relationships

System objectives: The system's primary objective is to provide assurance to the homeowner. This is achieved by the system's ability to detect and alert the homeowner, SecurityCo.com, and proper authorities of a disruption(s) in the system that may result in an undesired event taking place. Below are the three objectives of the system:

- Assure
- Detect
- Alert

System elements:

1. Home elements
 - Control panel: Wireless module control panel
 - Door/window sensor
 - Smoke detector
 - Motion sensor
 - Mobile Device
 - VOIP phone adapter
 - Telephone
 - Personal computer
 - Internet (Home)
 - Electricity (Home)

2. External elements

- 2 Way radio network
- SecurityCo.com network
- Central monitoring station
- Customer notifications

System relationships: The system relationships are best shown in the Functional Block Diagram that is at the start of this section.

Part Four (1-4): Define the scope of the FMEA.**1. Definitions for system failure as it relates to system objectives:**

- The security system does not provide assurance to the homeowner.
- The security system detects an undesired event, but does not alert homeowner that an event has occurred or is occurring.
- The security system does not detect an undesired event, but alerts the homeowner that an event has occurred or is occurring.
- The security system does not detect an undesired event, and does not alert the homeowner that an event has occurred or is occurring

2. Types of causes to be considered:

- Accidental
- Random
- Deliberate
- Malicious

3. The nature of this analysis will primarily focus on a descriptive basis.**Part Five (1-5): Complete and file the FMEA pre-analysis worksheet and review it with the customer.**

Step 2: Identify Failure Modes

Part One (2-1): Identify the important functions of each system element. Consider the following questions:

Element	Purpose	System needs	Performance relationship	Single point of failure?
Control panel	Link between user and SecurityCo.com	To properly receive sensor data and communicate with SecurityCo.com server	The control panel needs to function correctly while the system is engaged	Yes
Door/window sensor	Detects ajar doors and windows	Send sensor data to the control panel to say whether the door is open or closed	Door/Window sensor must perform correctly or the system will receive false data	No
Smoke detector	Detect smoke/fire	To provide early detection from fire and to provide adequate time to exit the home.	The smoke detector must perform properly to assure homeowner.	No
Motion sensor	Detect motion	Detect any unwanted movement within the home	This is a redundancy measure to back up the door/window sensors	No
Mobile device	Means of communication between SecurityCo.com and customer	The system needs to communicate a detection with the mobile device	The performance of the system is reliant on communicating a disruption in the system to the homeowner.	No
VOIP phone adapter	Provides homeowner with Voice Over IP telephone and DSL Internet	VOIP is a secondary means for communication between homeowner and SecurityCo.com	The performance of the system is reliant on communicating a disruption in the system to the homeowner.	No
Telephone	Means of communication between SecurityCo.com and customer	VOIP Telephone communication is a means for alerting the homeowner	The performance of the system is reliant on communicating a disruption in the system to the homeowner.	No
Personal computer	Means of communication between SecurityCo.com and customer	DSL Internet allows the user to receive communication via E-mail or over the PC's speaker system	The performance of the system is reliant on communicating a disruption in the system to the homeowner.	No
Internet (Home)	Connects through the VOIP phone adapter to provide Internet and Telephone to the homeowner.	The system needs the Internet to send and receive data on the status of the home.	The system will perform without the Local Network due to redundancy in communication.	No

Element	Purpose	System needs	Performance relationship	Single point of failure?
Electricity (Home)	Provides energy to the home and the security system.	The system requires this element to provide the home with electricity.	The system is reliant on the home's source of electricity. There are no backup power sources in place.	Yes
2-Way radio network	Links communication between the home Control Panel and SecurityCo.com Network Operations Center	The system requires this element to maintain successful link between two elements	The system is reliant on the success of this element.	Yes
SecurityCo.com (NOC)	Communicates the home's security status with SecurityCo.com and the homeowner.	System requires element to communicate proper information received by the Control Panel.	The system is reliant on the success of this element.	Yes
Central monitoring station	Communicates the home's security status with SecurityCo.com.	System requires element to communicate proper information received by the Control Panel to SecurityCo.com staff	The system is reliant on the success of this element.	Yes
Customer notification	Communicates the home's security status with homeowner.	System requires element to communicate proper information received by the Control Panel to homeowner	The system is reliant on the success of this element.	Yes

Part Two (2-2): Identify all plausible ways failure could happen for each system element.

For Part 2-2 we applied Divergent-Convergent Thinking to identify potential events that could cause the security system to fail. The screenshot below shows the potential failure modes of the Control Panel.

1. Loss of power
2. Sends incorrect sensor data
3. Faulty programming

Control Panel: Plausible Failures

Baseline Failure Modes and Effects Analysis											
System: Home Security System				FMEA Analyst: Ryan M. Dewar				Last Update: 4/24/2010			
Element: Control Panel				Notes: Insert notes here							
ID	Potential Failure Mode	Potential Effects of Failure	S E V	Postulated Cause		O C C	Prognostic Capabilities		D E F T	R P N	
1	Loss of power	What are the consequences of failure?		What could cause failure?			What warning capabilities are there?				
2	Sends incorrect sensor data										
3	Faulty programming										
15											
16											
17											
18											
19											

Step 3: Estimate Effects of Failure and their Severity Rating

This step estimates system-level effects corresponding to the occurrence of each failure mode.

Part One (3-1): Identify all the consequences of each failure mode identified in Part 2 of Step 2. In this step there may be multiple effects that could occur due to the failure of each element. For this example we have identified two effects of failure that apply to the Control Panel. These effects are shown in the following figure.

1. Full system failure leads to intrusion
 2. False alarm leads to end-user aggravation

Control Panel: Effects of Failure

Baseline Failure Modes and Effects Analysis											
System: Home Security System				Last Update: 4/24/2010							
Element: Control Panel				FMEA Analyst: Ryan M. Dewar							
Notes: Insert notes here											
ID	Potential Failure Mode	Potential Effects of Failure	S E V	Postulated Cause		O C C	Prognostic Capabilities			D E T	R P N
Unique ID	How can this system element fail?	What are the consequences of failure?		What could cause failure?			What warning capabilities are there?				
1	Loss of power	Full system failure; Intrusion									
2	Sends incorrect sensor data	Triggers false alarm; End-user aggravation									
3	Faulty programming	Full system failure; Intrusion									
4	Faulty programming	Triggers false alarm; End-user aggravation									
13											
14											
15											
16											
17											
18											
19											

Note: We have added a fourth potential failure mode during this step, because if the Control Panel's operating system contains faulty programming the potential effects of this event could lead to Full system failure leads to intrusion or False alarm leads to end-user aggravation.

Part Two (3-2): Estimate the seriousness of each effect. This is the severity rating, or SEV.

Specifically, SEV answers the following question:

How severe of an impact would be the outcomes following the occurrence of a particular failure mode?

To further define our definitions of severity, we have expanded the Severity Levels table to meet the specific needs of this analysis. In the table below these definitions have been provided.

Severity		
Rating	Description	Definition
10	Severely High	Everything of value was stolen or destroyed
9	Extremely High	Value of items stolen or destroyed was greater than \$5000
8	Very High	Value of items stolen or destroyed was greater than \$2500
7	High	Value of items stolen or destroyed was greater than \$1000
6	Moderate	Significant decrease in customer assurance, No damage
5	Low	Decrease in customer assurance, No damage
4	Very Low	Minimal decrease in customer assurance, No damage
3	Minor	No decrease in customer assurance, No damage
2	Very Minor	Random inconvenience, No damage
1	None	Failure had no consequence

Control Panel: Severity Levels

Step 4: Identify Potential Causes of Failure and Estimate their Likeliness

This step seeks to identify the reasons why failure of system elements might occur.

Part One (4-1): Determine all potential root causes for each failure mode. Included in this portion of the analysis are a number of potential causes for the failure of the Control Panel element of the security system. Some of the causes fall under the category of accidental, random, as well as deliberate and malicious. The image below depicts where this step should be completed within the FMEA Workbook.

Control Panel: Potential Root Causes

Baseline Failure Modes and Effects Analysis

System: Home Security System
Element: Control Panel
FMEA Analyst: Ryan M. Dewar
Notes: Insert notes here
Last Update: 4/24/2010

ID	Potential Failure Mode	Potential Effects of Failure	Postulated Cause	Prognostic Capabilities		Downtime
				S E V	O C C	
Unique ID	How can this system element fail?	What are the consequences of failure?	What could cause failure?		What warning capabilities are there?	
1	Loss of power	Full system failure: Intrusion	Wires intentionally severed			
2	Loss of power	Full system failure: Intrusion	Weather related power outage			
3	Loss of power	Full system failure: Intrusion	Blow fuse			
4	Loss of power	Full system failure: Intrusion	Power accidentally turned off			
5	Loss of power	Full system failure: Intrusion	Random system malfunction			
6	Loss of power	Full system failure: Intrusion	Control panel intentionally turned off by intruder.			
7	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	Overcooked food sets off smoke detector			
8	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	Control panel incorrectly communicating with sensors			
9	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	Intruder intentionally causes the system to send "false alarms"			
11	Faulty programing	Triggers false alarm: End-user aggravation	Careless or disgruntled employee			
12	Faulty programing	Full system failure: Intrusion	Careless or disgruntled employee			
13	Faulty programing	Triggers false alarm: End-user aggravation	Bugs in code			

Part Two (4-2): Estimate the likelihood of occurrence for each root cause. This is the occurrence rating, or OCC. Specifically, OCC answers the following question: *What is the likelihood that the particular failure mode caused by the particular failure mechanism will occur?*

To further define our definitions of occurrence, we have expanded the Occurrence Levels table to meet the specific needs of this analysis. In the table below these definitions have been provided.

Occurrence		
Rating	Description	Definition
10	Very High	Event will occur constantly
9	High	Event occurs daily
8	High	Event occurs monthly
7	High	Event occurs yearly
6	Moderately High	Event is common and likely
5	Moderate	Event is common
4	Moderately Low	Event is common and unlikely
3	Low	Event is uncommon
2	Low	Event is uncommon and unlikely
1	Remote	Unlikely

Control Panel: Occurrence Levels

SecuritySystem_FMEA_Workbook [Compatibility Mode] - Microsoft Excel

File Home Insert Page Layout Formulas Data Review View

PivotTable Table Picture Clip Shapes SmartArt Screenshot Column Line Pie Bar Area Scatter Other Charts Sparklines Line Column Win/Loss Slicer Filter Links

M12

Baseline Failure Modes and Effects Analysis Last Update: 4/24/2010

System: Home Security System FMEA Analyst: Ryan M. Dewar

Element: Control Panel Notes: Insert notes here

ID	Potential Failure Mode	Potential Effects of Failure	S	E	P	C	O	C	R	G	D	E	P	T	N
			What could cause failure?	What warning capabilities are there?											
1	Loss of power	Full system failure: Intrusion	10	Wires intentionally severed	2										
2	Loss of power	Full system failure: Intrusion	10	Weather related power outage	4										
3	Loss of power	Full system failure: Intrusion	10	Blow fuse	4										
4	Loss of power	Full system failure: Intrusion	10	Power accidentally turned off	6										
5	Loss of power	Full system failure: Intrusion	10	Random system malfunction	2										
6	Loss of power	Full system failure: Intrusion	10	Control panel intentionally turned off by intruder	2										
7	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	1	Overcooked food sets off smoke detector	4										
8	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	5	Control panel incorrectly communicating with sensors	3										
9	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	5	Intruder intentionally causes the system to send "false alarms"	2										
11	Faulty programming	Triggers false alarm: End-user aggravation	5	Careless or disgruntled employee	2										
12	Faulty programming	Full system failure: Intrusion	10	Careless or disgruntled employee	2										
13	Faulty programming	Triggers false alarm: End-user aggravation	5	Bugs in code	5										
14		Central monitoring station		Customer notification											
15				Control Panel (2)											

Step 5: Estimating Detection and its Effectiveness

Part One (5-1): Identify current failure detection capabilities. In this illustrated example we have identified certain failure detection mechanisms that SecurityCo.com already has in place. Specifically, the figure below displays the failure detection mechanisms in place for the Control Panel.

Control Panel: Failure Detection Capabilities

Baseline Failure Modes and Effects Analysis										Last Update: 4/24/2010	
System: Home Security System				FMEA Analyst: Ryan M. Dewar							
Element: Control Panel				Notes: Insert notes here							
ID	Potential Failure Mode	Potential Effects of Failure	S E V	Postulated Cause	O C C	Prognostic Capabilities			D E T	R P N	
Unique ID	How can this system element fail?	What are the consequences of failure?		What could cause failure?		What warning abilities are there?					
1	Loss of power	Full system failure: Intrusion	10	Wires intentionally severed	2	SecurityCo.com "Loss of Power" Customer Notification					
2	Loss of power	Full system failure: Intrusion	10	Weather related power outage	4	SecurityCo.com "Loss of Power" Customer Notification					
3	Loss of power	Full system failure: Intrusion	10	Blow fuse	4	SecurityCo.com "Loss of Power" Customer Notification					
4	Loss of power	Full system failure: Intrusion	10	Power accidentally turned off	6	SecurityCo.com "Loss of Power" Customer Notification					
5	Loss of power	Full system failure: Intrusion	10	Random system malfunction	2	SecurityCo.com "Loss of Power" Customer Notification					
6	Loss of power	Full system failure: Intrusion	10	Control panel intentionally turned off by intruder	2	SecurityCo.com "Loss of Power" Customer Notification					
7	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	1	Overcooked food sets off smoke detector	4	Allow a response "window" for user to shut off smoke alarm					
8	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	5	Control panel incorrectly communicating with sensors	3	Test system's validity regularly					
9	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	5	Intruder intentionally causes the system to send "false alarms"	2	If "false alarms" are a persistent issue, have system tested by					
11	Faulty programming	Triggers false alarm: End-user aggravation	5	Careless or disgruntled employee	2	Test system's validity regularly					
12	Faulty programming	Full system failure: Intrusion	10	Careless or disgruntled employee	2	Test system's validity regularly					
13	Faulty programming	Triggers false alarm: End-user aggravation	5	Bugs in code	5	Test system's validity regularly					

Part Two (5-2): Estimate the ability to warn about the onset of failure. This is detectability rating, or DET. Specifically, DET answers the following question:

What is the likelihood that the onset of failure will be detected in enough time to do something about it?

Detectability			
Rating	Description	Rating	Description
10	Absolute Uncertainty	5	Moderate
9	Very Remote	4	Moderately High
8	Remote	3	High
7	Very Low	2	Very High
6	Low	1	Almost Certain

Control Panel: Detectability Levels

Baseline Failure Modes and Effects Analysis

Last Update: 4/24/2010

ID	Potential Failure Mode	Potential Effects of Failure	S E V	Postulated Cause	O C C	Prognostic Capabilities		R P N
						What could cause failure?	What warning capabilities are there?	
1	Loss of power	Full system failure: Intrusion	10	Wires intentionally severed	2	SecurityCo.com "Loss of Power"	1	
2	Loss of power	Full system failure: Intrusion	10	Weather related power outage	4	SecurityCo.com "Loss of Power"	1	
3	Loss of power	Full system failure: Intrusion	10	Blow fuse	4	SecurityCo.com "Loss of Power"	1	
4	Loss of power	Full system failure: Intrusion	10	Power accidentally turned off	6	SecurityCo.com "Loss of Power"	1	
5	Loss of power	Full system failure: Intrusion	10	Random system malfunction	2	SecurityCo.com "Loss of Power"	1	
6	Loss of power	Full system failure: Intrusion	10	Control panel intentionally turned off by intruder.	2	SecurityCo.com "Loss of Power"	1	
7	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	1	Overcooked food sets of smoke detector	4	Allow a response "window" for user to shut off smoke alarm	1	
8	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	5	Control panel incorrectly communicating with sensors	3	Test system's validity regularly	1	
9	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	5	Intruder intentionally causes the system to send "false alarms"	2	If "false alarms" are a persistent issue, have system tested by	1	
11	Faulty programing	Triggers false alarm: End-user aggravation	5	Careless or disgruntled employee.	2	Test system's validity regularly	1	
12	Faulty programing	Full system failure: Intrusion	10	Careless or disgruntled employee.	2	Test system's validity regularly	1	
13	Faulty programing	Triggers false alarm: End-user aggravation	5	Bugs in code	5	Test system's validity regularly	1	

Step 6: Summary and Follow-On Analysis

This step determines a rank order of failure modes and summarizes the analysis in the form of a FMEA table.

Part One (6-1): Calculate the risk priority number. The risk priority number is labeled RPN and results from the product $SEV \times OCC \times DET$. Also, calculate Criticality by multiplying severity by occurrence, $SEV \times OCC$. These numbers provide guidance for ranking potential failures in the order they should be addressed. This step, however, is not required to be done in this manner, and may be substituted with simple Sorting, Weighted Ranking, or augmented using quantitative risk analysis methods.

Control Panel: Detectability Levels

Baseline Failure Modes and Effects Analysis

Last Update: 4/24/2010

ID	Potential Failure Mode	Potential Effects of Failure	S E V	Postulated Cause	O C V	Prognostic Capabilities		D E R T
						What could cause failure?	What warning capabilities are there?	
1	Loss of power	Full system failure: Intrusion	10	Wires intentionally severed	2	SecurityCo.com "Loss of Power"	1 20	
2	Loss of power	Full system failure: Intrusion	10	Weather related power outage	4	SecurityCo.com "Loss of Power"	1 40	
3	Loss of power	Full system failure: Intrusion	10	Blow fuse	4	SecurityCo.com "Loss of Power"	1 40	
4	Loss of power	Full system failure: Intrusion	10	Power accidentally turned off	6	SecurityCo.com "Loss of Power"	1 60	
5	Loss of power	Full system failure: Intrusion	10	Random system malfunction	2	SecurityCo.com "Loss of Power"	1 20	
6	Loss of power	Full system failure: Intrusion	10	Control panel intentionally turned off by intruder.	2	SecurityCo.com "Loss of Power"	1 20	
7	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	1	Overcooked food sets of smoke detector	4	Allow a response "window" for user to shut off smoke alarm	1 4	
8	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	5	Control panel incorrectly communicating with sensors	3	Test system's validity regularly	1 15	
9	Sends incorrect sensor data	Triggers false alarm: End-user aggravation	5	Intruder intentionally causes the system to send "false alarms"	2	If "false alarms" are a persistent issue, have system tested by	1 10	
11	Faulty programing	Triggers false alarm: End-user aggravation	5	Careless or disgruntled employee.	2	Test system's validity regularly	1 10	
12	Faulty programing	Full system failure: Intrusion	10	Careless or disgruntled employee.	2	Test system's validity regularly	1 20	
13	Faulty programing	Triggers false alarm: End-user aggravation	5	Bugs in code	5	Test system's validity regularly	1 25	

Part Two (6-2): Complete the baseline FMEA table. For most practical systems requiring a FMEA, it is common to generate a lot of paper. Be sure to organize the FMEA in a manner that lends itself to providing the needed information quickly.

Part Three (6-3): Develop actions for consideration. Such actions include:

The most common failure mode that exists in the SecurityCo.com security system is the potential loss of power at various points in the system.

- The recommendation we have made is to incorporate system emergency back-up power supplies in three locations (The home, 2-way radio tower, and the SecurityCo.com Center of Operations). These redundant power supplies will significantly reduce the chances of failure in the system.

Part Four (6-4): Is this failure mode associated with a critical characteristic? The failure mode is not associated with a critical characteristic.

Part Five (6-5): Periodically revisit and revise the FMEA as changes are made. Remember, FMEA is a living analysis, and as such every so often the analysis should be looked at again to identify any changes in the system or operational environment.

This page is intentionally blank.

APPENDIX J. FAULT TREE ANALYSIS

What is it? Fault Tree Analysis (FTA) is a top-down approach for identifying how an undesirable event can happen or be made to happen. A Fault Tree systematically breaks down a single undesirable event in terms of its potential underlying causes.

Variants on the FTA methodology include Success Tree Analysis ([J.3.2](#)), which instead focuses on a desired event occurring, and Attack Tree Analysis ([J.3.1](#)), which also considers malicious events resulting from the interaction of vulnerabilities, threats (exploits) and countermeasures.

-
- Why use it?**
- **Educate analyst on system details** - The act of constructing a fault tree will help analysts and stakeholders learn the fine details of how a particular system works. In many cases, stakeholders only have an appreciation for the success of the overarching system and not the smaller sub-systems, which make a system work. This is dependent on the tree having an understanding of the whole system, instead of one specific area. The interaction of all areas of a system is critical.⁴⁴
 - **Identifies scenarios** - FTA helps decision makers identify what data or situations to monitor to assist with preempting the occurrence of failure. The visual representation of logic aids in understanding how basic and intermediate events lead to the top event.
 - **FTA can be used to prioritize** - The fault tree helps to prioritize the contributors leading to the top event. When determining how to allocate resources and costs, the fault tree can provide value by displaying redundancies or single point of failure events.
-

- Timing** Assess Phase analytic activities:
- Common cause analysis
 - Design change evaluation
 - Accident / incident analysis
 - Risk assessment
 - Identification of safety / security critical components
- FTA should be used when one requires knowing how high-level failure events of interest could occur (such as for a system) in response to failure of lower level events (such as components of a system). FTA should only be used when the system can be explicitly described (such as for an engineered system) and when the manner in which elements of system interact is known. In contrast, if the system is difficult to describe, the components of a system are unknown, or act in unpredictable or unknown ways, FTA would be difficult if not impossible to complete. However, attempting to construct a fault tree for such unascertained systems might yield useful insights.

⁴⁴ Long, Allen R. "Beauty and the Beast - Use and Abuse of the Fault Tree as a Tool." Fault Tree Analysis and Probabilistic Risk Assessment. <<http://www.fault-tree.net/presents-html/beauty/title.html>>.

Steps	The FTA methodology is comprised of the following nine steps: Step 1: Define an event of interest as the top event of the fault tree Step 2: Define the next levels of the tree Step 3: Develop questions to examine the credibility of the branches Step 4: Gather data to answer questions Step 5: Determine whether the branch is credible Step 6: Determine whether the branch is sufficiently developed Step 7: Stop branch development Step 8: Stop when the scenario model is complete Step 9: Identify causal factors
Tips	<p>Final product may be incomplete - When presenting a fault tree to a decision maker or other analysts, failure to show a single event that is readily known to the decision maker or analysts may influence the perceived credibility of the product. A general untested rule of thumb is as follows: <i>The proportion of missing sources of trouble is proportional to the number of things I can think of that are missing multiplied by a measure of my general familiarity of the system... that is, if I don't know much but still can detect something missing, then this fault tree representation is quite incomplete.</i> To avoid this problem, to the maximum extent possible, engage your client and collaborators throughout the process of constructing a fault tree.</p> <p>A fault tree's benefit is limited - A fault tree is only as good as the information and expertise used to create it. In the end, a fault tree will produce an exact logic model for a system, but that logic model will only be accurate to the extent that the user was correctly informed and knowledgeable about the system's true behavior.</p> <p>Avoid bias toward simplicity - While simple fault trees are relatively easy to construct and evaluate by hand, more complicated fault trees that must account for common cause failures or other types of dependencies require mathematical software to process. It is often tempting to ignore dependencies in the interest of keeping the fault tree simple, but in so doing the analyst might lose sight of potentially significant failure modes.</p> <p>Follow the logic not the diagram - It is possible to have two distinctly different looking fault trees that produce the same logic for the top event in terms of basic events. Thus, it is necessary to fully evaluate whether or not two dissimilar looking logic trees are logically equivalent. This can be done using truth tables for small fault trees, but larger fault trees require the use of mathematical software (e.g., Windchill FTA). .</p> <p>Be aware of sensitivity of probabilities - The manner in which a fault tree is presented may have an influence on the perceived probability of the top event⁴⁵. In particular:</p> <ul style="list-style-type: none"> • The perceived importance of a particular branch of a fault tree may increase depending on whether it was presented in pieces • People were quite insensitive

⁴⁵ Fischhoff, Baruch, Paul Slovic, and Sarah Lichenstein. "Fault Trees: Sensitivity of Estimated Failure Probabilities to Problem Representation." *Journal of Experimental Psychology: Human Perception and Performance*. Vol. 4, No. 2. May 1978, pp. 330-344.

Know your audience - It is important to know who the fault tree will be made for. The level the tree gets taken to depends on it. A tree that goes down to the deepest level may go beyond what is necessary. This will help keep the tree manageable.

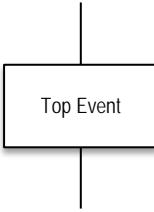
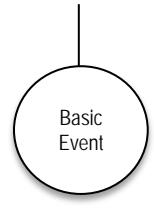
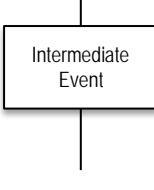
Consistent Nomenclature - The success of the fault tree hinges on consistent labeling of gates and events. Consistency allows you to compare sets of failure (cut sets) for symmetry

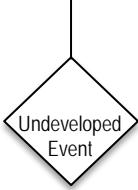
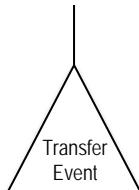
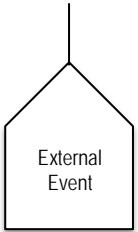
J.1. FTA SYMBOLS AND NOMENCLATURE

The following describes the standard symbols and terms used for constructing a fault tree.

J.1.1. Simple Events

All events in a FTA are characterized as Failure Events. This means that each event can take on one of two states: Failed or Not Failed. There are five generic types of events commonly used in FTA: the top event, basic events, intermediate events, undeveloped events, and transfer events.

Simple Events	Description
	<p>The Top Event defines the focus of the fault tree. Typically, the top event represents a particular type of failure of concern to a stakeholder. It is common for a risk study to focus on the occurrence or non-occurrence of this top event. The top event is typically denoted by a rectangular box placed at the top of a fault tree and connects to the fault tree only from the bottom (the output of a logic gate feeds into it).</p>
	<p>Basic Event is the lowest-level events of practical interest to the problem. Basic events interact with other events to cause failure at higher levels. Basic events are typically denoted by circles and connect to the fault tree only from the top (feeds into logic gates).</p>
	<p>Intermediate Events are events that result from the interaction of basic events but are lower level than the top event. It is common to use intermediate events to make a fault tree easier to read and interpret. Intermediate events are typically denoted with rectangular boxes connected to logic gates at the input and output.</p>

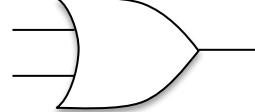
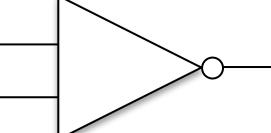
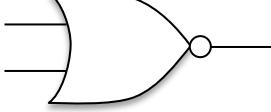
Simple Events	Description
 Undeveloped Event	Undeveloped Events are events that could, in principle, be decomposed further, but for various reasons the analyst decided not to do this. In practice, an undeveloped event is treated like a basic event until it is further developed. When an undeveloped event is developed, it becomes an intermediate event. Undeveloped events are typically denoted with diamonds connected to logic gates at the output.
 Transfer Event	Transfer Events are events that represent the top event from a separate fault tree. In practice it is treated as a basic event in the fault tree in which it appears, though it would actually be an intermediate event if one were to attach the referenced fault tree. Given that many real fault trees are very complex and detailed as a whole, transfer events are typically used to organize and present the entire tree in a manner that could be easily read and understood. Transfer events are typically denoted with a triangle connected to logic gates at the output.
 Conditioning Event	Conditioning Event is one that imposes a conditional restriction on any logic gate. For example, a conditioning restriction might be applied to an OR gate which tells it to default to “Not Failure” regardless of the state of its inputs unless the conditioning event occurs. In practice, conditioning events are used to facilitate communication among analysts, but could be easily replaced with a suitable combination of AND and OR gates. A conditioning event is typically denoted by an oval.
 External Event	External Event is one that is known to occur or not occur. For example, an external event might be a specific decision made, action taken, or switch flipped. An external event is typically denoted by a symbol shaped like a house.

J.1.2. Logic Gates

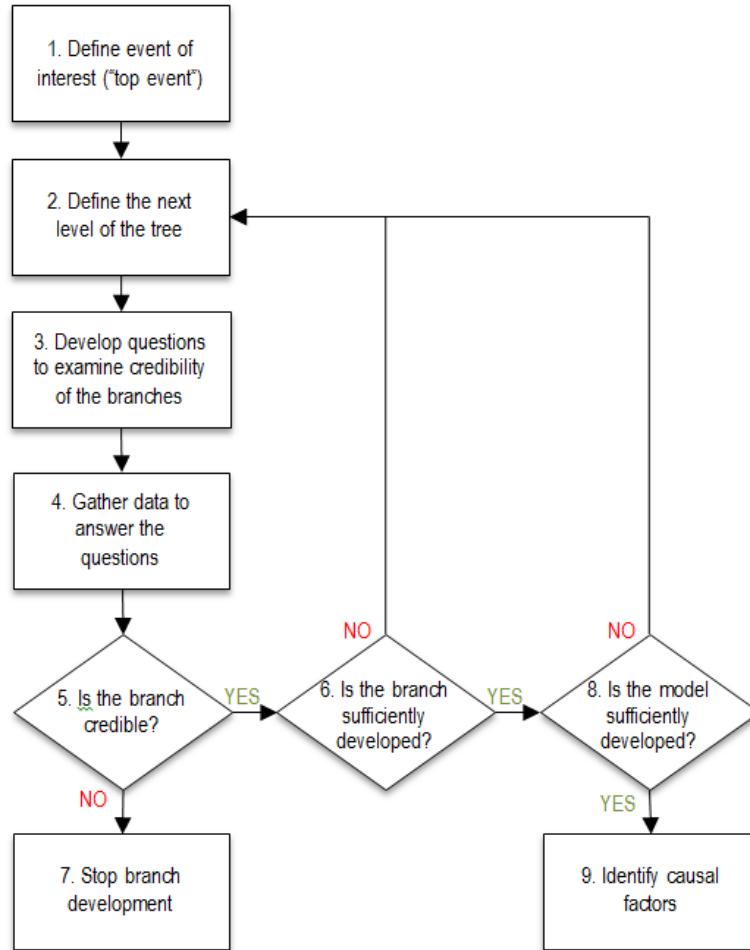
A logic gate in FTA describes how lower-level events interact with one another to produce higher-level events. Typically, two or more events (basic, intermediate, undeveloped, or transfer) feed into a gate from the bottom. The corresponding inputs to the gate are either the event occurred (i.e., failure occurred, failed, or simply “True”) or the event did not occur (i.e., failure did not occur or simply “False”). Depending on the logic associated with the gate, the output from the gate feeds into the top event or an intermediate event from the top, where the output is failure (“True”) or not failure (“False”).

Note: In the case of success trees, the same logic applies with the exception that the event “Success” is used in place of “Failure.”

The five most commonly used types of logic gates are the AND gate, OR gate, NOT gate, XOR gate, and INHIBIT gate.

Logic Gate	Description	Symbol
AND Gate	An AND gate outputs “Failed” if all the inputs to the gate represent failure. Otherwise, the AND gate returns “Not Failed.”	
OR Gate	An OR gate outputs “Failed” if one or more inputs to the gate represent failure. Only if all inputs represent “Not Failed” does an OR gate return “Not Failed.”	
NOT Gate	A NOT gate outputs the state that is opposite that of the input. NOT gates receive only one input. For example, if the input is “Failed,” a NOT gate returns “NOT Failed.”	
NAND (Not and) Gate	The NAND gate is a digital logic gate that works inversely to the AND logic. If one or both inputs are LOW, a HIGH output results. The NAND gate is a universal gate in the sense that any Boolean function can be implemented by NAND gates.	
NOR (Not or) Gate	The NOR gate is a HIGH output (1) results if both the inputs to the gate are LOW (0). If one or both input is HIGH (1), a LOW output (0) results. NOR is the result of the negation of the OR operator. NOR is a functionally complete operation and combinations of NOR gates can be combined to generate any other logical function.	
XOR (Exclusive or) Gate	An XOR gate outputs “Failed” if only one of the inputs represents failure (and all others represent success). If more than one input represents failure, the XOR gate returns “Not Failed.” XOR is semantically equivalent to the way in which the word “OR” is used in common speech.	
INHIBIT Gate	An INHIBIT gate outputs “Failed” if all input events represent failure AND a conditional event also occurs. An INHIBIT gate will return “Not Failed” if either one or more inputs represent “Not Failure” or the conditioning event does not occur.	

J.2. FAULT TREE ANALYSIS: PROCESS STEPS⁴⁶



Step 1: Define an event of interest as the top event of the fault tree.

Clearly describe a specific, known event or condition of interest for which you will explore the potential underlying causes. Failed performance of a countermeasure, overall system, or policy are types of top events. An objective loss event such as “structural damage” or “financial ruin” can also be the top event. It is often helpful to preface this step by describing the system under study in terms of its objectives, state variables, inputs, and outputs (see System Description Methodology, [Appendix W](#)).

The top event needs to be specifically and clearly defined because it determines the scope of the FTA. A loss event definition that includes only the immediate consequences, results in recommendations that are fairly narrow in scope. A loss event definition that also includes subsequent consequences of the incident, results in recommendations that are broader in scope.

Multiple loss events may be identified as part of a single investigation. Multiple loss events are usually needed when there are different types of consequences or when the consequences affect different stakeholders. When this occurs, multiple fault trees may be used – each corresponding to a different loss

⁴⁶ Rooney, James J., Lee N. Vanden Heuvel, Donald K. Lorenzo, and Laura O. Jackson. “Cause and Effect: Fault Tree Analysis Assesses What Leads to an Event.” *Quality Progress*. February 2009, p.p. 38-44.

event or stakeholder perspective. However, in many cases, events and conditions from one fault tree will feed into other fault trees; consequently, there will be dependency among the fault trees.

Step 2: Define the next levels of the tree.

Determine the combinations of events and conditions that can cause the event to occur or the condition to exist.

If a number of events or conditions (e.g., two or more) must occur to cause the event, use an “AND” gate and draw the events or conditions under the “AND” gate. For example, for a release of hazardous chemicals to occur, the pipe carrying hazardous chemicals and the containment system must both fail.

If faced with the following situations, an “AND” gate would be used in the fault tree:

- Multiple elements must be present for an event to occur or a condition to exist.
- Multiple pathways must all be in specific states for an event to occur or a condition to exist.
- Redundant equipment items must all fail for an event to occur or a condition to exist.
- Safeguards must fail for an event to occur or a condition to exist.

If there are multiple potential ways for an event to occur, use an “OR” gate. If faced with the following situations, an “OR” gate would be used in the fault tree:

- One or more multiple elements cause an event to occur or a condition to exist.
- Failure of one or more parts of a system causes it to fail.
- Any one or more of several pathways in a specific state causes an event to occur or a condition to exist.

Regardless of whether an “AND” or an “OR” gate is selected, this level of development should be the smallest logical step (within reason) - a baby step toward the underlying potential causes of the event or condition above it. Taking too large a step can lead to important possibilities being overlooked.

Try to group components or actions by function. These high-level functions allow baby steps as the tree is developed. These small steps also allow testing of many possibilities with a single test. Remember to include equipment problems, human errors, and external events as appropriate.

As each item is added to the tree, test the logic. Start with each event or condition at the bottom of the tree.

Does the logic of the tree reflect your understanding of the event or condition of the system?

If an event or condition is connected to an “AND” gate above it, all the events or conditions connected to the “AND” gate must occur or exist for the event or condition above to occur or exist. If only one of the inputs is needed, then the “AND” gate logic is not correct.

If an event or condition is connected to an “OR” gate above it, then each event or condition connected to the “OR” gate must be enough, on its own, to cause the event or condition above. If a combination of two or more inputs is needed, then the “OR” gate logic is not correct.

Step 3: Develop questions to examine the credibility of the branches.

This step helps with knowing how to use the fault tree for monitoring a given situation. For example:

- What evidence would be present if this branch was true?
- What data should be missing if this branch was true?

- What data would demonstrate this branch is false?

Remember, you do not have to be a technical subject-matter expert for the analysis. Use the expertise of others to help you develop the fault tree structure and apply the data to assess each branch appropriately.

Step 4: Gather data to answer questions.

Gather data to answer the questions that were generated in the previous step. Data may include both tangible data and testimonial data.

Step 5: Determine whether the branch is credible.

Use the data gathered in the previous step to determine which branches of the tree are valid (i.e., true because they happened or are present) and which are invalid (i.e., false because they did not happen or were not present).

Ask questions such as:

- Does the data support or disprove the credibility of this branch?
- Do you have sufficient information to determine whether the branch is valid? If you do not, you need to gather more data or continue to develop the next level of the tree.

Cross out any branches that can be dismissed with high confidence and list the specific data used to make the determination beneath or next to the crossed-out item.

If all branches leading to the event or condition through an “OR” gate are eliminated, or if one or more branches leading to the event or condition of interest through an “AND” gate are eliminated, one of the following occurred:

- The event or condition of interest (the effect) did not occur or exist
- The event or condition of interest (the effect) did occur or exist and some of the data is inaccurate or was misplaced.
- Other ways exist for the event or condition of interest (the effect) to occur/exists

Determine whether the branch is credible. If the branch is credible, continue to step 6. If the branch is not credible, proceed to step 8.

Step 6: Determine whether the branch is sufficiently developed.

The branch is complete when it is detailed enough to show how the top event or condition occurred or existed, and causal factors can be identified.

If the branch is not complete, return to step 2. If the branch is complete, move on to step 8.

Step 7: Stop branch development.

If you have determined the branch is not valid, there is no reason to develop it further. Stop development of this branch and move on to step 8.

Step 8: Stop when the scenario model is complete.

The model is complete when you clearly understand how the top event or condition occurred or existed, and causal factors can be identified.

Keep the model just adequate for identifying issues of concern for your analysis. Avoid unnecessary detail or resolution that will not affect results or recommendations. If there is more than one possible way for the event of interest to have occurred and you cannot gather data to dismiss any of the remaining possibilities, consider each as a potential causal factor and make recommendations to prevent each possible way the event may have occurred. Conversely, if the data appears to dismiss all the events, then the model is not complete. Revise the model to include additional possibilities.

Step 9: Identify causal factors.

If the fault tree method is being used as the primary analysis tool, causal factors should be identified. Remember, causal factors are equipment, policy, or personnel performance gaps.

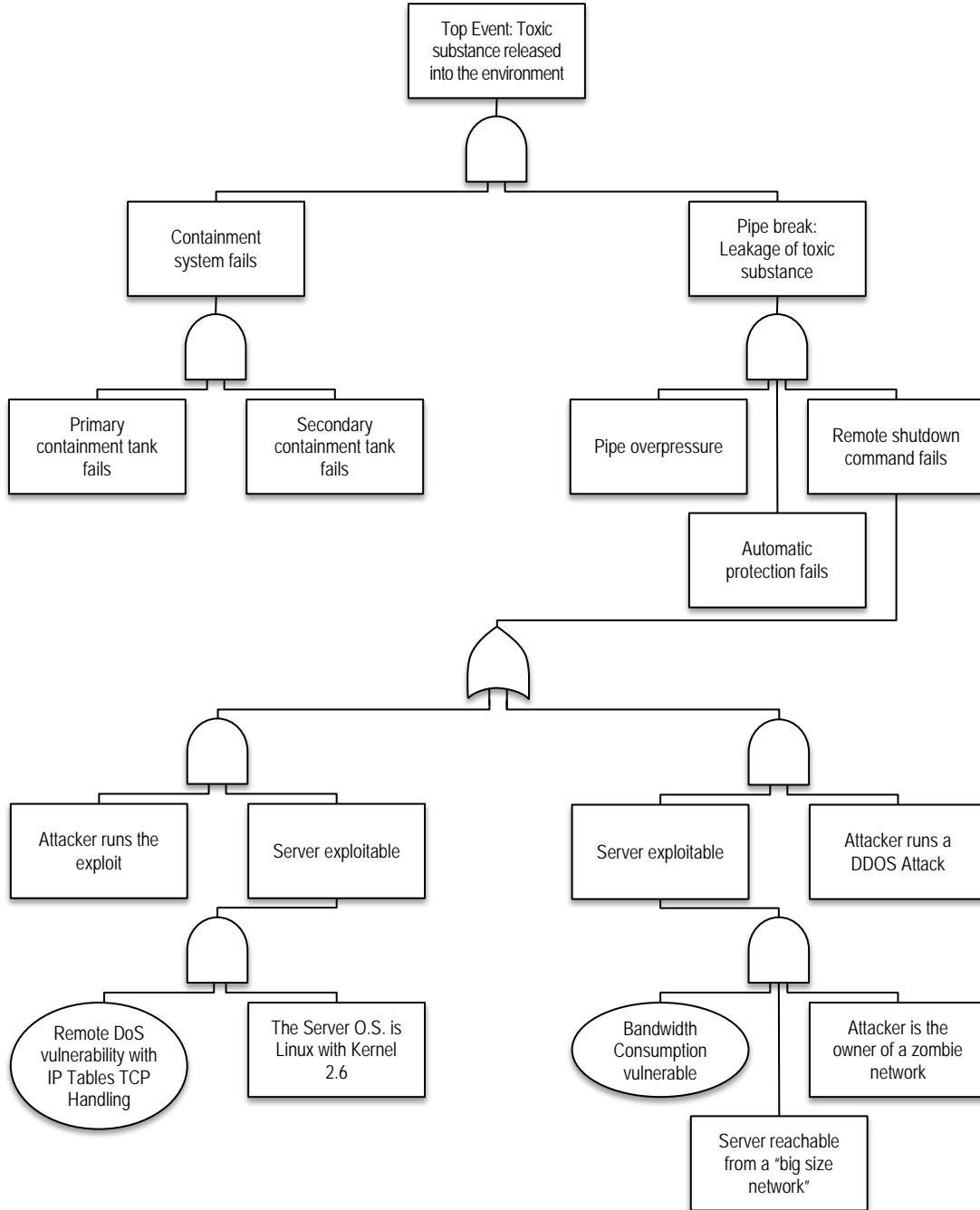
Subsequent Analysis

Traditional FTA is often accompanied by the identification of cut sets. A cut set represents a set of failure modes (basic events) that would result in the occurrence of the top event, if they were to all occur. In general, a fault tree can be simplified to a small set of intermediate events formed by combining sets of basic events with an AND gate (cut set), then combining these intermediate events with an OR gate to produce the top event.

J.3. ILLUSTRATIVE EXAMPLE

Example: Hybrid fault tree/attack tree

This example shows a hybrid fault tree/attack tree where the top event represents a release of toxic chemical.⁴⁷ This hybrid tree shows how random failures and attacker actions can interact to cause the top event.



⁴⁷ Fovino, Igor N., Marcelo Masera, Alessio De Cian. "Integrating Cyber Attacks within Fault Trees." *Reliability Engineering and System Safety*. Vol. 94. September 2009, pp. 1394-1402. <https://www.cert.fi/attachments/hvk-materiaali/automaatio/5llaj2pjf/ress4142_final.pdf>

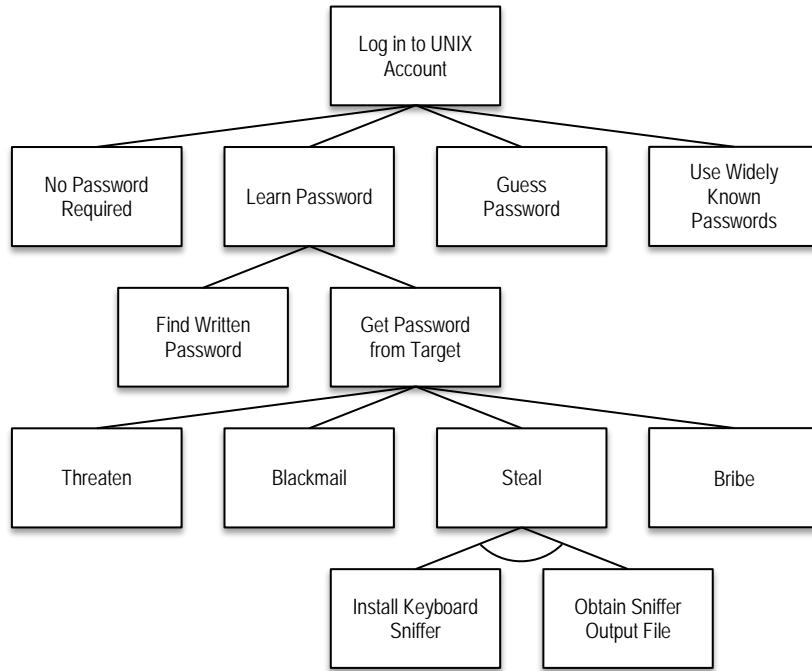
According to this tree, there are four high level scenarios of concern. The two extreme scenarios are described as follows:

- Purely Random Failure: Pipe overpressure exceeds limits, the automatic protection and remote shutdown command function fails, and both the primary and secondary containment tanks fail.
- Attacker Controlled Failure: Pipe overpressure exceeds limits, automatic protection fails, the remote shutdown command function fails due to a successful denial of service attack, and both primary and secondary containment are destroyed by explosives.

J.3.1. Attack Tree Analysis

An attack tree is a type of fault tree that includes both traditional basic events (e.g., accidental, random) and malicious events resulting from the combination of threats and vulnerabilities. It is okay to refer to fault trees that include random, accidental, and maliciously-induced failures as simply a fault tree.

The procedure for constructing an attack tree is identical to the procedure for constructing a fault tree with the exception that basic events include both vulnerabilities and its exploits (threats). Use guidance for developing a fault tree to also construct an attack tree.



The attack tree to log in to a UNIX account aids you in considering alternative ways in which a node can be achieved. Analysts are forced to ask themselves questions from an attacker's perspective, such as "How can I steal passwords?" By taking a broader view of information security, WebSphere Application Server security expands from permissions granted on an Enterprise Java Bean to the possibility of installing keyboard sniffers on WebSphere Application Server administrators' computers. This perspective is far different from a WebSphere developer's perspective for designing and building secure Enterprise Java Beans. Comprehensive WebSphere security encompasses more than the specific WebSphere Application Server application environment.

Enterprise architects, information system managers, system administrators, security experts, and WebSphere team members must consider additional aspects of vulnerabilities and penetration points that computer attackers can exploit outside of the WebSphere framework. Attack tree analysis offers a systematic methodology for identifying penetration points and system vulnerabilities not considered from the application design perspective.⁴⁸

J.3.2. Success Tree Analysis

Success Tree Analysis (STA) is a top-down approach for identifying how a desirable or successful event can happen or be made to happen. An alternative approach is Fault Tree Analysis (prior pages of [Appendix J](#)) that focuses on an undesired or failure event occurring.

A success tree is the logical complement of a fault tree. That is, given a fault tree with a top event (e.g., “Bad Thing Happens”), the success tree can be obtained by taking the negation of this top event (resulting in “Bad Thing Does Not Happen”). The simplest way to construct a success tree is to treat the top event of the complementary fault tree as an intermediate event and append a NOT gate to the output.

The procedure for constructing a success tree is identical to the procedure for constructing a fault tree with the exception that events are geared toward success (the “TRUE” state) as opposed to failure. See the methodology article on Fault Tree Analysis for more information.⁴⁹

⁴⁸ Pallas, Michael S. “Attack Trees: It’s a Jungle out There.” The Business Forum. <<http://www.bizforum.org/whitepapers/candle-4.htm>>.

⁴⁹ McGill, William L. The Pennsylvania State University. 2010.

This page is intentionally blank.

APPENDIX K. HAZARD AND OPERABILITY ANALYSIS

What is it? Hazard and Operability Analysis (HazOp) is a bottom-up approach that identifies potential hazards and operability complications within a system. This structured and systematic technique is used for examination and risk management.⁵⁰ This team-based analysis is used to identify potential hazards and operability issues associated with a system that cause it to deviate from its designed intent. The assumption is that a team of experts with different backgrounds can together produce greater results than the same experts working independently on the same analysis.

As a risk assessment tool, HazOp is often described as:

- A qualitative risk assessment tool
- A quantitative risk assessment tool
- A brainstorming technique
- An inductive risk assessment tool where success relies on the ability of the subject-matter experts (SMEs)

Why use it? One of the greatest benefits that HazOp offers is that it is helpful when dealing with hazards that are difficult to quantify. Typically within complex organizations and systems there are hazards that are difficult to detect, analyze, or isolate. By taking a less quantitative approach, this methodology does not force its users to apply explicit measurements, probabilities, or severity – which allows them to identify new ways to identify things that would usually be viewed as immeasurable such as human performance and behaviors.

The HazOp approach also provides industries that typically apply quantitative methodologies with a simplistic approach that relies more on intuition. Through the team oriented process, HazOp provides users with a built-in brainstorming process which potentially helps to catch some areas of concern that may be missed otherwise

Timing Develop, Define, and Assess Phases: HazOp is best used when there is uncertainty surrounding the risks and vulnerabilities of a facility, equipment, or process. This methodology enables SMEs to assess a system from multiple perspectives – making it one of the most commonly used of its kind. Some of the perspectives which can be analyzed include:

- **System Design:** HazOp can help assess system design capabilities to meet the users' specifications and safety standards as well as provide early detection for weaknesses in a system.
- **Physical and operational environments:** HazOp can certify that a system is fulfilling its designed intent (i.e., ensuring the system is appropriately situated, supported, and services contained, etc.)

⁵⁰ *The HAZOP (Hazard and Operability) Method*. AcuTech Process Risk Management. <http://www.acusafe.com/Hazard_Analysis/HAZOP_Technique.pdf>.

- **Operational and procedural controls:** Assessing engineered controls (e.g., automation), sequences of operations, procedural controls (e.g., human interaction), etc., and assessing different modes – start-up, standby, normal operation, steady and unsteady states, normal shutdown, emergency shutdown, etc.

Steps	The HazOp method is comprised of the following four steps: <ol style="list-style-type: none"> 1. Definition 2. Preparation 3. Examination 4. Documentation
Tips	<ul style="list-style-type: none"> • HazOp provides no means to assess hazards involving interactions between different parts of a system or process. • HazOp provides no risk ranking or prioritization capability. Teams may optionally build-in such capability as required, using a variety of methods. • HazOp provides no means to assess effectiveness of existing or proposed controls (e.g., safeguards). May need to interface HazOp with other risk management tools to support this level of analysis.

K.1. HAZOP STEPS

Step 1: Definition

Part One (1-1): Define purpose, scope, objectives. The purpose, scope, and objectives' of a HazOp analysis are typically developed by the decision maker(s) within an organization. The overarching purpose of HazOp is to identify hazards and operability problems within a system, but it is important to identify, in more detail, the true purpose for engaging in this analysis.

Being able to do this will help in narrowing the scope of the project and achieving a finite list of objectives.

Some examples that have been used in prior engagements include:

- Check the safety of a design
- Decide whether and where to build
- Develop a list of questions to ask a supplier
- Check operating/safety procedures
- Improve the safety of an existing facility
- Verify that safety instrumentation is reacting to best parameters.

It is also important to define what specific consequences are to be considered:

- Employee safety (in plant or neighboring research center)
- Loss of plant or equipment
- Loss of production(lose competitive edge in market)

- Liability
- Insurability
- Public safety
- Environmental impacts.

Part Two (1-2): Team selection. It is important to select a group of experts from various disciplines with the appropriate skills and experience to successfully complete the analysis. The individuals selected should also display additional characteristics such as strong intuition and good judgment, this is because during a HazOp the team members will encounter situations where they will not be able to apply finite numbers or probabilities but instead use qualitative measures or ranges.

Typically a team consists of five to seven members although a smaller team could be sufficient depending on the scope of the project. The team should also select a strong team leader who has experience applying a HazOp or applying a similar group oriented methodology. This leader will be required to keep the team focused on identifying problems, because unless the problems have a simple solution, the purpose of this analysis is not necessarily to solve them.

Part Three (1-3): Define responsibilities. In project planning it is important to assign individual responsibilities to each of the members participating in the study. This is desired by planners, because it reduces the risk of finger-pointing later on through the project lifecycle.

Step 2: Preparation

The preparation steps taken in HazOp are similar to the processes found in product lifecycle management processes. A team member with project management experience would be a valuable asset in this step of the process.

Part One (2-1): Plan Study. The planning process is used to determine how the product team will conduct their analysis. Some of the attributes of a study to consider are the following:

- Design of the study
- How the study will be validated
- Tool used to perform the study

Part Two (2-2): Collect Data. Data collection requires the team members to collect the proper data to perform their examination of the system. This could be done by using sensor data, survey tools, or observations.

Part Three (2-3): Agree on style of recording. When planning a team project it is important to agree on the style of recording, so that each individual can benefit from the analysis that is being performed. Some questions to ask during this step are:

- Will we write a lengthy report?
- Will we use graphs and charts to visualize results?
- Will bullets be used?

Part Four (2-4): Estimate the timelines for analysis. Any project now follows a timeline in which certain deliverables of the project are met at certain times to ensure all stakeholders that their commitment

to the project and their expectations are being satisfied. With a mix of team members with various experiences, it is possible to build adequate estimates for each phase of the project.

Part Five (2-5): Arrange schedule. Once you have determined the time estimations of the project you can plot a schedule for the completion of the deliverable. It is important to include buffers in this schedule for steps of the project that may take longer than others.

Step 3: Examination

Examining a system needs to be an iterative process. Once Part 3-1 is completed, this portion of HazOp must be repeated until each of the system's parts has been analyzed.

Part One (3-1): Divide the system into parts. Dividing the system into its parts, if it has never been done before, can be an extremely revealing process.

This step will allow you to see all of the intricate parts of a system as well as the subsystems working within a system. It may be beneficial in this process to apply a Reliability Block Diagram ([Appendix R](#)) to gain a graphical view of the system and its parts.

Part Two (3-2): Select a part and define design intent. Each part of a system must complete a certain task in order to complete the system's objective(s). You may find that some parts of the system exist solely for redundancy purposes; others may provide essential functions that without them a system will fail.

Part Three (3-3): Identify deviation by using guide words on each element. By applying Guide Words to each element of the system you are able to communicate its importance to the system in terms that can be understood by all of the members of a team. As the table below shows there are ways of communicating both Quantitative and Qualitative meaning to the elements.

The most popular feature of the HazOp methodology is the “Guide-Word” approach. The use of guidewords allows the group of SMEs to have a common language and understanding when they discuss risk. There are many variations of this approach specialized for particular industries.

Guide Word	Meaning
No	Negation of the design intent
Less	Quantitative Decrease
More	Quantitative Increase
Part of	Qualitative Decrease
As Well As	Qualitative Increase
Reverse	Logical Opposite of the Intent
Other Than	Complete Substitution

Part Four (3-4): Identify consequences and causes. Once the system element has been well defined, the team can now identify some of the consequences and causes a malfunction of the element could cause to the entire system. These can be identified either by experience or past events or by other thinking exercises such as Divergent-Convergent Thinking ([Appendix C.3](#)).

Part Five (3-5): Identify whether a significant problem exists. By identifying potential causes and consequences, you are able to now identify if the element of the system being study has the ability to cause significant damage to the system. An existing tool, that is used to identify the logical failure of a system, is known as a Fault Tree Analysis ([Appendix J](#)). This process, if used properly, can identify the chain or chains of events that would result in a system failure.

Part Six (3-6): Identify protection, detection and indicating mechanisms. If a significant problem or weakness does exist, there is now cause for action to ensure the element's failure will not result in system failure or measures can be put in place for early detection of this element's failure. Divergent-Convergent Thinking ([Appendix C.3](#)) again is an excellent thinking tool to help identify potential solutions, but creating the solution is outside of the scope of this analysis unless it is agreed upon as a "simple fix."

Part Seven (3-7): Identify possible remedial/mitigating measures (Optional).

Part Eight (3-8): Agree on actions. Finally, in Step 3, the team must agree on the necessary or recommended action to reduce the risks that have been identified by this analysis.

Part Nine (3-9): Repeat Steps 3-2 to 3-8. Remember the first iteration of this process only analyzes one element of the system. Some of the system parts may be completed quickly; others may take much longer depending on their importance to the overall system.

Step 4: Documentation

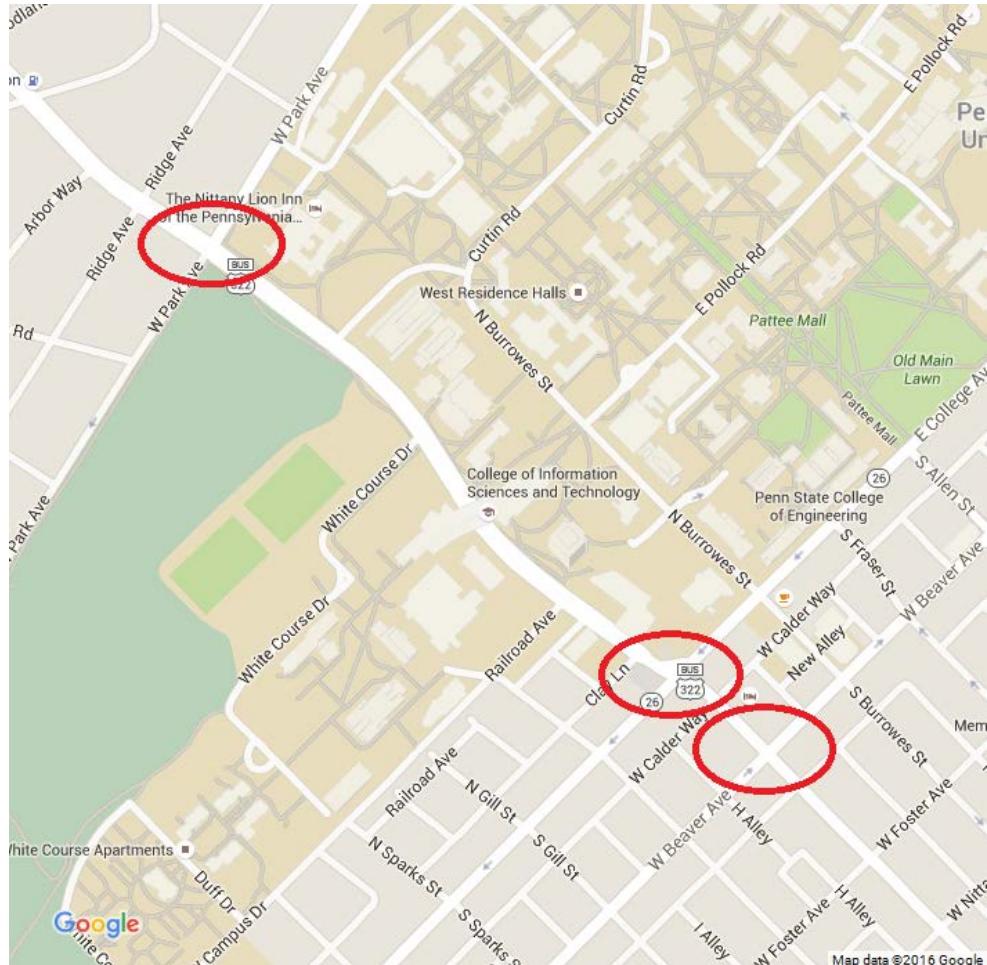
There are many different ways to document an analysis. The following bullets are simply a guideline to completing the reporting for the HazOp analysis. It is important to follow the reporting guidelines that were agreed upon in Step 2, Part 3.

- Record the examination
- Sign off the documentation
- Produce the report of the study
- Follow up that actions are implemented
- Re-study any parts of the system if necessary
- Produce the final output report

K.2. ILLUSTRATIVE EXAMPLE

The State College/University Park area is prone to traffic congestion along several main arteries. Utilizing a HazOp approach, assess the hazards and problems with efficient operation along these routes. The routes to be considered, shown in the diagram below, are Atherton St., Park Ave., College Ave., and Beaver Ave. The parts of concern, indicated below by ovals, are the intersections of these routes.

The traffic signal at these intersections are being investigated to determine whether the timing patterns are optimal during various times of day, and also during event traffic. The purpose of the signals is to guide the flow of traffic in such a manner that the time that any given vehicle spends within the specified area is minimized.



To apply the HazOp method, one must determine:⁵¹

- Keywords: Flow
- Part Location: The three intersections marked on the above diagram
- Deviation: No or Less
- Causes of deviation
- Consequences of deviation
- Safeguards against deviation
- Actions to take in response to a deviation

⁵¹ Lihou, Mike. "Hazard & Operability Studies (HAZOPS)." HAZOP Manager V6.0. n.d. <<http://lihoutech.com/hazop.htm>>.

This information can be tabulated in matrix form. A sample matrix for this particular example is shown below:

Keyword	Intersection	Deviation	Cause	Consequence	Safeguards	Action
Flow	Ath/Park	No	Collision	Significant Congestion	Speed Limit; No Turn on Red	Quick response by police/emergency services
Flow	Ath/Park	No	Event Traffic	Extreme Congestion	Mark additional exit routes	Traffic control officers
Flow	Ath/Park	Less	Rush Hour	Congestion	Signal coordination	Adjust signal timing for rush hour
Flow	Ath/Park	Less	Power Outage	Signals are ineffective	Generator Supply	Utilize generators, Traffic control officers
Flow	Ath/College	No	Collision	Significant Congestion	Speed Limit; No Turn on Red	Quick response by police/emergency services
Flow	Ath/College	Less	Rush Hour	Congestion	Signal coordination	Adjust signal timing for rush hour
Flow	Ath/College	Less	Move-in Traffic	Congestion	Clearly mark parking/entrance routes	Stagger move-in times; traffic control officers
Flow	Ath/College	Less	Move-out Traffic	Congestion	Clearly mark exit routes	Traffic control offices
Flow	Ath/College	Less	Power Outage	Signals are ineffective	Generator supply	Utilize generators, Traffic control officers
Flow	Ath/Beaver	No	Collision	Significant Congestion	Speed Limit; No Turn on Red	Quick response by police/emergency services
Flow	Ath/Beaver	Less	Rush Hour	Congestion	Signal coordination	Adjust signal timing for rush hour
Flow	Ath/Beaver	Less	Move-in Traffic	Congestion	Clearly mark parking/entrance routes	Stagger move-in times; traffic control officers
Flow	Ath/Beaver	Less	Move-out Traffic	Congestion	Clearly mark exit routes	Traffic control officers
Flow	Ath/Beaver	Less	Power Outage	Signals are ineffective	Generator supply	Utilize generators, Traffic control officers

Using this HazOp matrix as a starting point, planning officials can prepare for congestion that may result from various causes. Data acquisition – monitoring the states of congestion during the identified “causes” – would be the next stage of the HazOp procedure. Additionally, planners may choose to model or test modified signal timings or other safeguards/responses based on the HazOp matrix and assess their effectiveness in mitigation congestion. After considering all relevant variables and response methods and their effects on traffic flow, planning officials will be able to reduce the magnitude and negative impact of congestion. In other words, the HazOp procedure will assist them in optimizing traffic flow in the event of any deviations.

This page is intentionally blank.

APPENDIX L. HIERARCHICAL HOLOGRAPHIC MODELING

What is it?	Hierarchical Holographic Modeling, or HHM, is a technique for examining an issue from multiple points of view. ⁵² HHM helps identify the various sources of risk present in a large-scale system. The product of an HHM analysis is a “hierarchy of holographies,” where each holography represents alternative perspectives one can take on an issue and its sub-issues.
Why use it?	<p>The exercise of developing an HHM generates useful and valuable insights, particularly if the issue or system is large and complex.</p> <p>It is often useful to leverage an HHM to systematically identify sources of risks from different viewpoints and perspectives. These risk scenarios can be later screened and filtered using a variety of techniques such as qualitative risk analysis or quantitative risk analysis.</p> <p>In addition, an HHM may also help planners design exercise scenarios based on a variety of situations that may occur during an all-hazards event.</p>
Timing	Assess Phase: HHM provides a tool useful for establishing a common operating picture of a particular issue, system, or question. HHM forces stakeholders to examine an issue from multiple points of view in attempt to identify and uncover all sources of risk, both conventional and novel, known and previously unknown.
Steps	<p>The HHM method is comprised of the following six steps.</p> <ol style="list-style-type: none">1. Identify and discuss the key risk issue2. Define head topics3. Define subhead topics4. Cross check subhead topics against others5. Review the HHM6. Summarize and report
Tips	<ul style="list-style-type: none">• The methodology does not necessarily produce mutually exclusive and collectively exhaustive alternatives.• The HHM is only as good as the information and expertise leveraged to create it. If non-experts or poor quality information is used to develop the HHM, the credibility of the HHM is in question.• An HHM should only go as deep as is needed to easily identify sources of risk or concern pertaining to the key risk issue. In many cases, you need not break down or decompose all head topics to the same level; that is, just because you are very specific or general for one head topic does not require you to be equally specific elsewhere.

⁵² Haimes, Yacov Y. *Risk Modeling, Assessment, and Management*. Hoboken: John Wiley & Sons, 2009. Print.

L.1. HIERARCHICAL HOLOGRAPHIC MODELING STEPS

Materials and Initial Setup

The materials and resources needed to construct an HHM include:

- 5-7 individuals with complementary experiences related to the key risk issue under study
- A comfortable conference room, office or meeting space that can accommodate all participants
- Whiteboard with whiteboard (non-permanent) markers and eraser or a flat surface with multicolored sticky notes (e.g., Post-It notes) and a pen
- A facilitator dedicated to this activity or one that also serves as a participant
- A scribe dedicated to this activity or one that also serves as a participant
- One hour to 90-minutes of dedicated attention to this task
- Drawing or diagramming software (e.g., Visio, Omnigraffle, PowerPoint) for drawing the final HHM

Step 1: Identify and Discuss the Key Risk Issue

The key risk issue defines the basis for the HHM. Write this key risk issue on the board for all participants to see and read. A key risk issue may take the form of a question, keywords that allude to a system, or a topic of interest.

Allow some time for each participant to think about the issue and ask questions about the meaning of the words used, scope of the study, etc. Revise the issue statement as needed to improve clarity, refine its meaning or restrict its scope.

Step 2: Define Head Topics

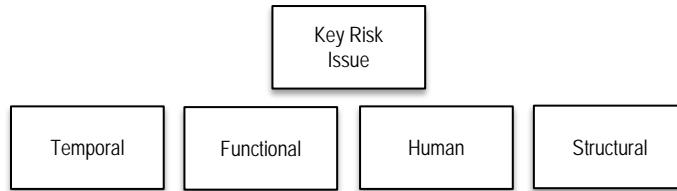
For the key risk issue identified, brainstorm as many different perspectives one could take in looking at the issue. In this context, a perspective represents a point of view one might take to examine the issue. For example, one might look at an issue in terms of its:

- Temporal aspects (e.g., time factors, events)
- Functional aspects (e.g., functions that a system serves)
- Human aspects (e.g., roles, responsibilities)
- Structural aspects (e.g., parts of a system)

One might treat each of these perspectives as individual head topics or perhaps decompose one of these into a more specific set of head topics. The choice is at the discretion of the participants.

For each head topic identified, draw a box containing a few keywords that characterize the perspective.

Draw all head topic boxes in a horizontal row across the top of a whiteboard or other writing surface (e.g., flat surface with sticky notes). It is often helpful to place the key risk issue in a box centered above the head topics, though this is not required. The result should look similar to the following:



Step 3: Define Subhead Topics

Systematically examine each head topic in turn and break each down further into multiple subhead topics.

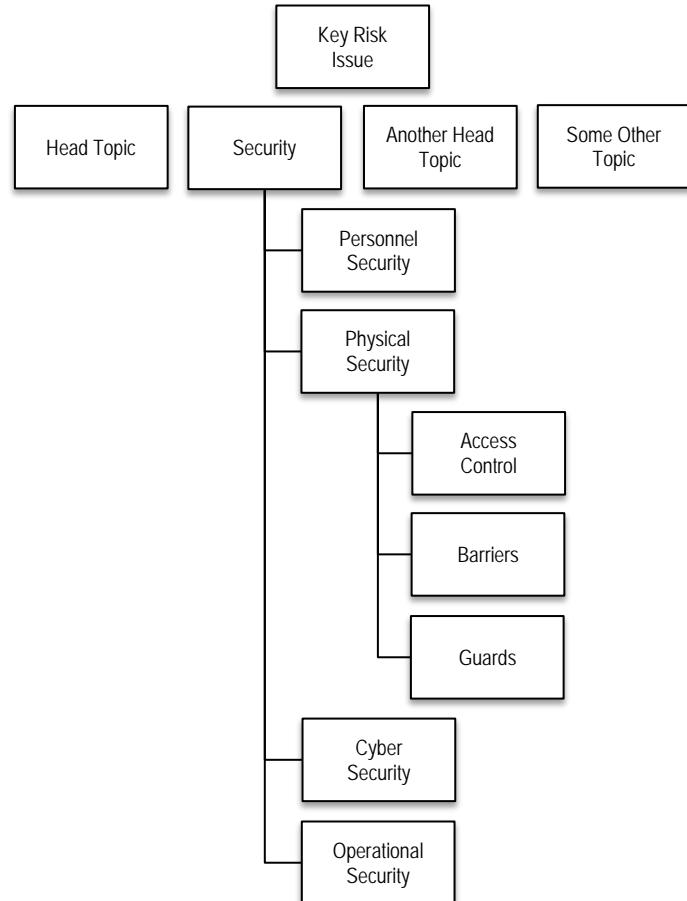
A subhead topic represents a different perspective one could take from a point of view constrained by the associated head topic.

For example, if the head topic is “Structural Aspects,” subhead topics might be “Hardware,” “Software,” “Human,” “Organizational,” and so on, where each represents a perspective one could take when looking at the issue from the “Structural” point of view.

- As another example, if the head topic is “Security,” subhead topics might be “Personnel,” “Physical,” “Cyber,” “Operational,” and so on.

Repeat this step as needed until you achieve the desired level of specificity for each head topic. That is, after you break down each head topic into subhead topics, you may further break down each subhead topic into even more narrow points of view.

Draw each subhead topic below the associated head topics, and arrange them vertically downward. The result should look similar to the figure below. You may or may not use the lines to connect subhead topics to head topics, though such connections are helpful for quickly grasping a multilevel HMM (i.e., one with greater than levels).



Step 4: Cross Check Subhead Topics Against Others

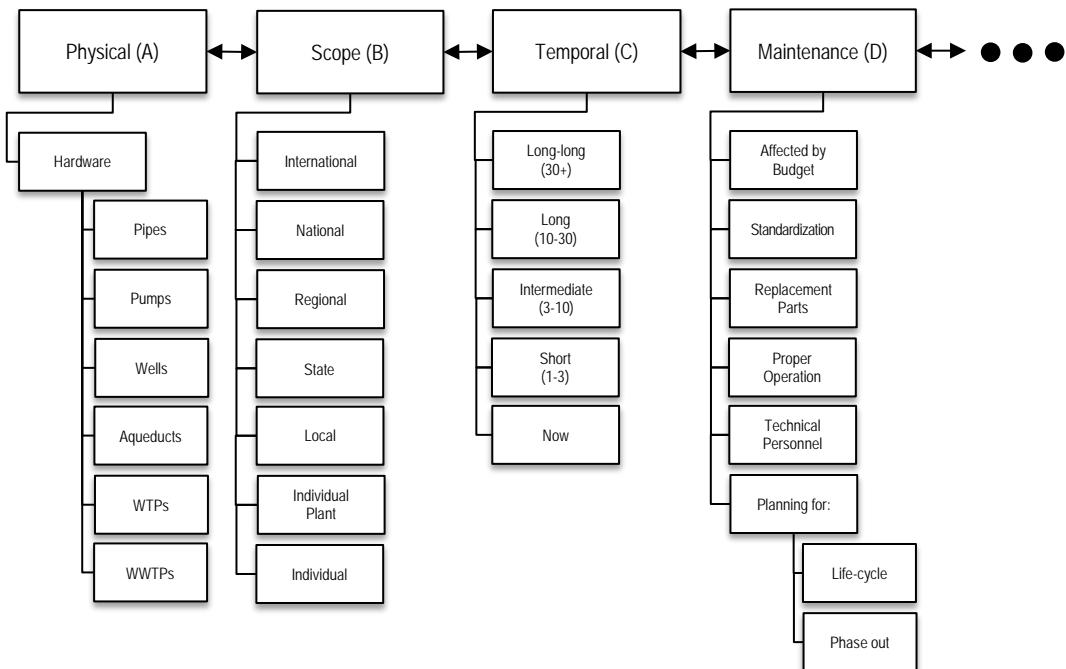
Systematically revisit each subhead topic identified and ask yourself whether it has relevance elsewhere.

Step 5: Review the HHM

After HHM subtopics have been cross checked against other categories, this step asks each participant to review the HHM to ensure that each perspective was adequately covered – whether additional perspectives need to be covered, etc. For example, during the review process, participants might ask:

- Are some perspectives redundant in whole or in part? If so, can they be merged or repackaged?
- Can this HHM be created another way? If so, how would it be different, and what can be done with the present HHM to minimize these differences?
- Are additional perspectives needed?
- Are the subhead topics adequately covered, or do they need to be expanded further?

To the maximum extent practical, given available resources, try to use this opportunity to improve the HHM. Note all pertinent observations in the final report, whether they are incorporated into the final HHM or not. An example of a finished HHM that examines the different perspectives on the issue of hardening a water supply system is provided below.⁵³



⁵³ Haimes, Yacov Y. *Protection of Critical Complex Transportation Infrastructures*. Transportation Research Board Committee A. 19 March 2001. <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.5123&rep=rep1&type=pdf>>

Step 6: Summarize and Report

This final step develops a final report that documents the HHM construction process and provides the final results. At a minimum this report should contain:

- The names of the persons involved in the HHM construction process.
- A clear statement of the key risk issue, to include any points helpful in resolving ambiguities about its meaning
- A schematic of the HHM and all of its detail
- A summary description of each head topic and subhead topic

Subsequent Analysis

A complete HHM can be used to support the following subsequent analysis activities:

- Identify, rank, and screen risk scenarios.
- Educate other stakeholders on the full nature of a particular key risk issue.
- Design exercise scenarios based on a variety of situations that might occur during an emergency.

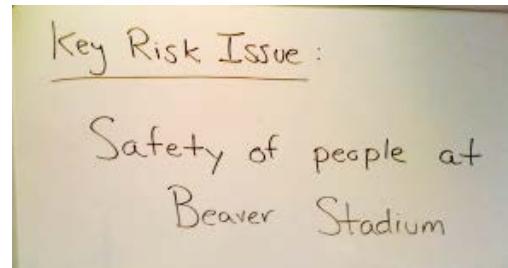
L.2. ILLUSTRATIVE EXAMPLE

This example develops an HHM for the following key risk issue: *Safety of persons attending an event at Beaver Stadium*

In the first step (Step 1) we wrote the key risk issue on the board and opened up the floor for discussion.

In particular, the following questions were asked:

- What do you mean by safety?
- Who are the people?
- Why focus on Beaver Stadium and not stadiums in general?
- What types of incidents are we including?



After the participants finished asking questions, we proceeded to identify a series of head topics (Step 2), each examined the issue of safety from different stakeholder perspectives, including:

- Attendees
- Administrative Staff
- Participants
- Emergency Services
- Pep Bands, Motivational Persons
- Vendors and Concession Workers
- Ushers

- Press
- Security
- Coordinators

For each head topic, we identified a series of subhead topics (Step 3) where each examined a different perspective on safety from the head topic point of view. For example, under the Participants head topic, we identified the following subhead topics:

- Weather
- Conditions of the field
- Attendee mood and behavior
- Physical placement (with respect to everything else in the stadium)
- Accessories
- Behavior of competition
- Hydration

As a group, we decided to limit ourselves to constructing a two-level HHM. In addition, we further refined the scope to include only safety issues during the event. Consequently, this refinement allowed us to remove the Administrative Staff head topic because we believed that this perspective was absorbed by either the attendees or coordinators.

After all head topics were broken down into subhead topics, we systematically walked through each (Step 4) to check for relevance of a subhead topic against others. During this step, we observed two distinctly different types of subhead topics:

- Those that directly affect the safety of the individuals characterized by the head topic (e.g., weather affecting participants). Associated subhead topics were noted with green boxes.
- Those that are tied to actions that affect the safety of others (e.g., weather hampering the ability of emergency services to respond). Associated subhead topics with purple boxes.
- Some subhead topics alluded to both of these. Rather than list these twice under a given head topic or decompose the subhead topic into a third level, we noted such topics with a purple and green double-lined box.



Once cross checking was finished, we reviewed the HHM (Step 5) to see if anything was missing, if too much was added, whether we could merge sections together, and so on. In particular, we asked ourselves:

- How could we have constructed the HHM differently?
- What would the University's President think? (a lateral thinking strategy)

- What would be different if we expanded the scope to include concerns of the adjacent residential population?
- Where are the crosscutting themes?

At the conclusion of this discussion, we settled on the final HHM shown below. However, we were careful to note all pertinent parts of our discussion, particularly as they relate to any insights generated from the review phase.



This page is intentionally blank.

APPENDIX M. INFLUENCE DIAGRAMS

What is it?	An Influence Diagram (also known as a relevance diagram, decision diagram, or a decision network) is a compact visual representation of a decision situation that shows how a set of variables interact with one another. The goal of an Influence Diagram is to offer insight into how system components such as decisions, uncertainties, and objectives influence each other. An added benefit of Influence Diagrams is that they provide a means of identifying and displaying components of a system using an intuitive graphical interface. Analysts may be able to develop detailed quantitative models that are based on highly-conceptual Influence Diagrams.
Why use it?	Influence Diagrams can help to create better understanding of any system. Through Influence Diagrams, a visual representation of the system being studied is produced. This visual representation helps individuals to better understand how a system is constructed, where the dependencies lie, and what the integral parts of the system are. Its objectively-visual nature also makes it conducive to communicating efforts, such as in presentations or thinking exercises.
Timing	Define Phase: Influence Diagrams offer an intuitive graphical representation of the relations between system components and are useful in situations that require mainly conceptual or abstract breakdowns of decision systems. Decision-making problems may be approached by analysts first in the context of an Influence Diagram, and then in more detailed quantitative models. An Influence Diagram may also provide an alternative to a decision tree; decision trees, by their nature, may branch boundlessly, while Influence Diagrams provide a more compact solution. In general, Influence Diagrams are useful when system components are interdependent, cause-and-effect relationships need to be articulated, or when simply mapping interpersonal relations provides a benefit to the analyst.
Steps	The overall approach for classifying events and data is comprised of three steps: <ol style="list-style-type: none">1. Identify the nodes2. Identify the relationships between the nodes3. Review the diagram
Tips	Clearly define variables. Typically, ineffective or inaccurate Influence Diagrams are characterized by improper definition of the variables and their relationships to one another. The arcs, used to connect the nodes in the diagram, generally indicate an influence. For instance, a decision node leading into a chance node indicates that the decision has a causal effect on the chance variable. Alternatively, chance nodes may lead to decision nodes. This does not indicate causality (as decision nodes are under the control of the decision maker), but rather temporal precedence. For example, a chance variable may occur which then leads to an action by a decision maker. In general, to properly use the method, care needs to be given when constructing the Influence Diagram such that causal and temporal relationships are correct and unambiguous.

It is also recommended that all variables within an Influence Diagram are both mutually exclusive and conditionally exhaustive. Failure to meet either or both of these criteria may produce a diagram which fails to accurately capture all facets of the decision problem.

When compared to a decision tree, an Influence Diagram proves a much simpler and compact depiction of analysis. Though the decision tree explains more details of the potential paths or scenarios as series of branches, this detail requires a lot of complex procedure, making it too complicated to display. While, the Influence Diagram illustrates the dependencies among variables more visibly than the decision tree.⁵⁴

M.1. INFLUENCE DIAGRAMS STEPS

Step 1: Identify the nodes

Part One (1-1): Begin by creating a list of all the nodes within the diagram. Nodes include anything which influences the final outcome and anything in a system that assists it in functioning. A Divergent-Convergent Thinking ([Appendix C.3](#)) exercise might assist in this process.

Part Two (1-2): For each node, determine the node type. Each type of node is given a unique appearance on the diagram in order to ease visual navigation of the diagram. The following is a list of node types, along with their standard shapes.

- Decision Nodes correspond to an event in which a person or a machine makes a decision based on information received. Decision nodes can also be determined by the input of other variables within the diagram. Decision nodes are drawn as rectangles.
- Uncertainty Nodes correspond to uncertainties that are chosen to be modeled in the diagram. The value of an uncertainty node is not known due to insufficient information; however, its value may become known in the future. The defining feature of an uncertainty node is that unlike a decision node, it cannot be controlled directly by the decision-maker. A subtype of uncertainty node is a deterministic node, which corresponds to a type of uncertainty, which may become deterministically known following the occurrence or understanding of other events or uncertainties. Uncertainty nodes are drawn as ovals and double-ovals, respectively.
- Value Nodes (or objectives) correspond to some object or state of being that is desirable. Usually, the decision maker is trying to find decisions that maximize or minimize the object. Value nodes are drawn as octagons, hexagons, or diamonds.

Step 2: Identify the relationships (arcs) between the nodes

Once the nodes have been determined, the next step involves systematically identifying how certain nodes influence other nodes. These influences are represented graphically by single-headed arrows known as arcs. The arc denotes an influence; the node at the tail of the arc influences the node at the head of the arc.

Begin with a single node (typically the last node in the series or the value nodes), and then identify which other nodes influence that node. “Influence” can include both positive and negative forces on that node.

⁵⁴ “Decision Making and Influence Diagrams.” DecisionCraft Inc. <<http://www.decisioncraft.com/dmdirect/decisionmaking.htm>>.

For each influencing node, draw a directional arc from that node to the node being considered (such as a value node). Repeat this process until all influences are determined. Below is a list of arc types. Begin with a single node (typically the last node in the series or the value nodes), and then identify which other nodes influence that node. “Influence” can include both positive and negative forces on that node. For each influencing node, draw a directional arc from that node to the node being considered (such as a value node). Repeat this process until all influences are determined. Below a list of are types.

- Functional arcs (ending in value node) indicate that one of the components of an additively separable utility function is a function of all nodes at their tails.
- Conditional arcs (ending in uncertainty node) indicate that the uncertainty at the arrow head is probabilistically conditioned on the tail nodes.
- Informational arcs (ending in decision node) indicate that the decision at the arrow head is made with the outcome of all tail nodes known beforehand.

Step 3: Review the diagram

Review all of the nodes, the relationships between the nodes, and the overall form of the Influence Diagram. Ensure that the diagram makes sense. Add or remove nodes or relationships as needed.

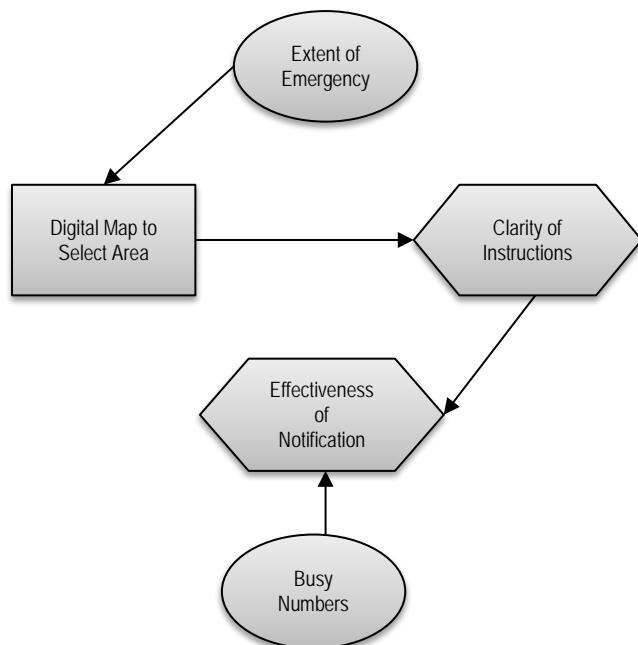
M.2. ILLUSTRATIVE EXAMPLE

The office of emergency communications for a U.S. county wants to assess the robustness of their emergency notification system. The purpose of the notification system is to provide telephone messages to residents in the event of an emergency. Members of the planning group meet to discuss the various aspects of the system, and elect to construct an Influence Diagram of the process. To add with the construction of the diagram, the group performs a Divergent-Convergent Thinking ([Appendix C.3](#)) exercise to come up with a list of any aspect that influences notifications being sent to residents during an emergency.

Step 1: Identify the nodes

The office of emergency communications for a U.S. county uses Influence Diagrams to assess the robustness of their emergency notification system, where they provide telephone messages to citizens. When they meet up, they use Divergent-Convergent Thinking ([Appendix C.3](#)) to come up with a list of everything that influences notifications being sent to residents during an emergency. The following is the list of nodes they came up with:

- Extent of Emergency
- Clarity of Instructions
- Notification



- Busy Numbers
- Digital Map

Once the list is finalized, the team discusses the type of node each represents. This is important, because the types of nodes are represented differently on the diagram. Here is the list of nodes accompanied by the type it represents:

- Extent of Emergency (Uncertainty)
- Clarity of Instructions (Value)
- Effectiveness of Notification (Value)
- Busy Numbers (Uncertainty)
- Digital Map (Decision)

Step 2: Identify the relationships between the nodes

After determining the nodes and node types, the team is able to construct the Influence Diagram. They start with “end” of the influence flow, or the value node which is of primary concern to the committee. This node, Effectiveness of Notification, is depicted in its representative shape (a hexagon).

From here, the team continues to construct the diagram by adding the nodes which influence Effectiveness of Notification. The group determines that Busy Numbers and Clarity of Instructions are the two nodes which influence Effectiveness of Notification, so they draw the two nodes (depicted by an oval and hexagon, respectively) with arcs pointing from each toward the Effectiveness node. The group continues this procedure until all nodes and influences have been exhausted. The final diagram, shown below, displays the flow of influence throughout the emergency notification procedure.

Step 3: Review the diagram

Once the team completes the diagram, they can review it and discuss whether it appropriately captures the aspects of influence within a system. The group may determine that relationships need to be refined or that nodes need to be added or deleted. In either case, the diagram would need to be redrawn and reanalyzed in an iterative procedure following these basic steps. After any adjustments are made, and the diagram is finalized, analysts may create more sophisticated models – models that are based on the Influence Diagram – to determine the effectiveness of the emergency notification system.

This page is intentionally blank.

APPENDIX N. MEASUREMENT OF INTANGIBLES

What is it?	The ability to assign quantitative measurement to characteristics that are generally believed to be immeasurable has been described in the book <i>How to Measure Anything: Finding the Value of Intangibles in Business</i> by Douglas W. Hubbard. By building on one of the cleverest thinkers in history, Nobel Prize winning physicist Enrico Fermi, Hubbard has constructed the Universal Measurement Method or Applied Information Economics Approach (AIE). Fermi who had a knack for intuitive and casual-sounding measurements, was famous for instilling in his students the ability to answer questions by approximating fanciful-sounding quantities that at first glance may seem immeasurable, through the use of existing knowledge. Questions similar to the example below are today commonly known as a “Fermi Question.” ⁵⁵
Why use it?	This method provides individuals with tools to estimate or apply ranges of qualitative or seemingly immeasurable characteristics, which in turn help to reduce uncertainty.
Timing	<p>Define and Assess Phases: This technique is designed to be used when an individual has the desire to reduce the uncertainty of an “intangible” or “immeasurable” characteristic that lacks quantitative data. Some example scenarios include:</p> <ul style="list-style-type: none">• Measuring with very small random samples (e.g., can you learn something from a small sample of potential customers, employees, and so on, especially when there is currently a great deal of uncertainty?)• Measuring the population of things that you will never see all of (e.g., the number of a certain type of fish in the ocean, the number of plant species in the rain forest, the number of production errors in a new product or of unauthorized access attempts in your system that go undetected, etc.)• Measuring when many other, even unknown, variables are involved (e.g., is the new “quality program” the reason for the increase in sales, or was it the economy, competitor mistakes, a new pricing policy, etc.?)• Measuring the risk of rare events (e.g., the chance of a launch failure of a rocket that has never flown before, or another September 11 attack, or another levee failure in New Orleans)• Measuring the value of art, free time, or reducing risk to your life by assessing how much people actually pay for these things.

⁵⁵ Hubbard, Douglas W. *How to Measure Anything: Finding the Value of “intangibles” in Business*. Hoboken: John Wiley & Sons, 2007. Print.

Steps The method for measuring intangibles is comprised of the following four steps:

1. Project Preparation
 - a. Preliminary research
 - b. Expert identification
2. Building a Decision Model
 - a. Decision problem definition
 - b. Decision model detail
 - c. Initial calibrated estimates
3. Preliminary Measurements
 - a. Value of information analysis (VIA)
 - b. Preliminary measurement method designs
 - c. Measurement methods
 - d. Updated decision model
 - e. Final value of information analysis
4. Metrics Design and Final Deliverable
 - a. Completed risk/return analysis
 - b. Identified metrics procedures
 - c. Decision optimization
 - d. Final report and presentation

Tips Many decision makers avoid trying to make observations because of a preconceived belief that a variety of obstacles exist that prevent measurement. Hubbard created a list of assumptions to help counter this belief

Four Useful Measurement Assumptions

1. Your problem is not as unique as you think: Chances are that the measurement you are attempting has been measured before either within the decision makers field or outside of their field
2. You have more data than you think: Typically the things you care about measuring are also things that leave tracks, making it possible to measure them.
3. You need less data than you think: Apply Hubbard's 'Rule of Five'
 - a. Rule of Five: There is a 93% chance that the median of a population is between the smallest and the largest values in any random sample of five from that population
4. There is useful measurement that is much simpler than you think: Assume that the first approach you think of is the hard way, and with a little more ingenuity, you can identify an easier way.

When creating estimate ranges for a measurement, humans by nature typically fall victim to their own overconfidence or underconfidence. Hubbard identifies when someone makes an estimate that their ranges should fall within a 90% Confidence Interval. This is to say that an estimator should have ninety percent confidence that any data point of a specific study would have a ninety percent chance of being within that range.

Unfortunately many of these estimates display signs of over or underconfidence.

- Overconfidence: When an individual routinely overstates knowledge and is correct less often than he or she expects. For example, when asked to make estimates with a 90% confidence interval, fewer than 90% of the true answers fall within the estimated ranges.

Underconfidence: When an individual routinely understates knowledge and is correct much more often than he or she expects. For example, when asked to make estimates with a 90% confidence interval, many more than 90% of the true answers fall within the estimated ranges.

N.1. MEASUREMENT OF INTANGIBLES STEPS

Step 1: Project Preparation

Part One 1-1: Preliminary research: Interviews, secondary research, and prior reports are studied so analyst can get up to speed on the nature of the problem.

Part Two 1-2: Expert identification: The process typically requires four or five experts who provide estimates, but as many as 20 have been included in the past.

Step 2: Build Decision Model

Part One 2-1: Decision problem definition: In a workshop setting, experts need to identify what specific problem they are trying to analyze. For example, are you trying to identify when the next terror attack will be, or is the real issue identifying areas where there may be holes in security? If the decision is an investment, project, commitment, or other initiative, then we need to have a meeting with decision makers to develop an investment boundary for the organization.

Part One 2-2: Decision model detail: By the second workshop, using an Excel spreadsheet, list all of the factors that matter in the decision being analyzed and show how they add up. If it is a decision to approve a particular major project, then you need to list all of the benefits and costs, add them into a cash flow, and compute a return on investment.

Part One 2-3: Initial calibrated estimates: In the remaining workshops, you calibrate the experts and fill in the values for the variables in the decision model. These values are not fixed points (unless you really know the values exactly). They are the calibrated expert estimates. All quantities are expressed as 90% confidence interval (CI) or other probability distributions.

Step 3: Preliminary Measurements

Part One 3-1: Value of information analysis (VIA): At this point you run a VIA on every variable in the model. This tells us the information values and thresholds for every uncertain variable in the decision. A macro written in Excel does this very quickly and accurately.

$$\text{Expected Value of Information (EVI)} = \text{Reduction in Expected Opportunity Loss (EOL)}$$

$$\text{EVI} = \text{EOL}_{\text{BeforeInfo}} - \text{EOL}_{\text{AfterInfo}}$$

Where $EOL = \text{chance of being wrong} \times \text{cost of being wrong}$

$$\text{Expected Value of Perfect Information (EVPI)} = \text{EOL}_{\text{BeforeInfo}} \text{ (EOL after } \emptyset \text{ if information is perfect)}$$

Part Two 3-2: Preliminary measurement method designs: From the VIA, you realize that most of the variables have sufficient certainty and require no further measurement beyond the initial calibrated estimate. Usually only a couple of variables have a high information value (and often they are somewhat of a surprise). Based on this information choose a measurement method that, while being significantly less than the Expected Value of Perfect Information (EVPI), should reduce uncertainty. The VIA also shows us the threshold of the decision. The measurement method is focused on reducing uncertainty at relevant threshold.

Part Three 3-3: Measurement methods: Decomposition, random sampling, subjective-Bayesian, controlled experiments, Lens models (and so on), or some combination thereof are all possible measurement methods used to reduce the uncertainty on the variables identified in the previous step.

Part Four 3-4: Updated decision model: You use the findings from the measurements to change the values in the decision model. Decomposed variables are shown explicitly in their decision model (e.g., an uncertain cost component may be decomposed into smaller components and each of its 90% confidence intervals are shown).

Part Five 3-5: Final value of information analysis: VIAs and measurements (the previous four steps) may go through more than one iteration, as long as the VIA shows a significant information value that is much greater than the cost of a measurement, measurement will continue. Usually, however, one or two iterations is all that is needed before the VIA indicates that no further measurements are economically justified.

Step 4: Metrics Design and Final Deliverable

Part One 4-1: Completed risk/return analysis: A final Monte Carlo simulation shows the probabilities of possible outcomes. If the decision is about some major investment, project, commitment, or other initiative, then compare the risk and return to the investment boundary for the organization.

Part Two 4-2: Identified metrics procedures: There are often residual VIAs (variables with some information value that were not practical or economical to measure completely, but would become obvious later on). Often these are variables about project progress or external factors about the business or economy. These are values that need to be tracked because knowing them can cause mid-course corrections. Procedures need to be put in place to measure them continually.

Part Three 4-3: Decision optimization: The real decision is rarely a simple “yes/no” approval process. Even if it were, there are multiple ways to improve a decision. Now that a detail model of risk and return has been developed, risk mitigation strategies can be devised and the investment can be modified to increase return by using what-if-analysis.

Part Four 4-4: Final report and presentation: The final report includes an overview of the decision model, VIA results, the measurements used, the position on the investment boundary, and any proposed ongoing metrics or decision optimization methods.

N.2. ILLUSTRATIVE EXAMPLE

The value of the system that monitors your drinking water: The use of Applied Information Economics Approach was used in an actual project, used to measure the benefits that came to the EPA’s Safe Drinking Waters Information System (SDWIS).

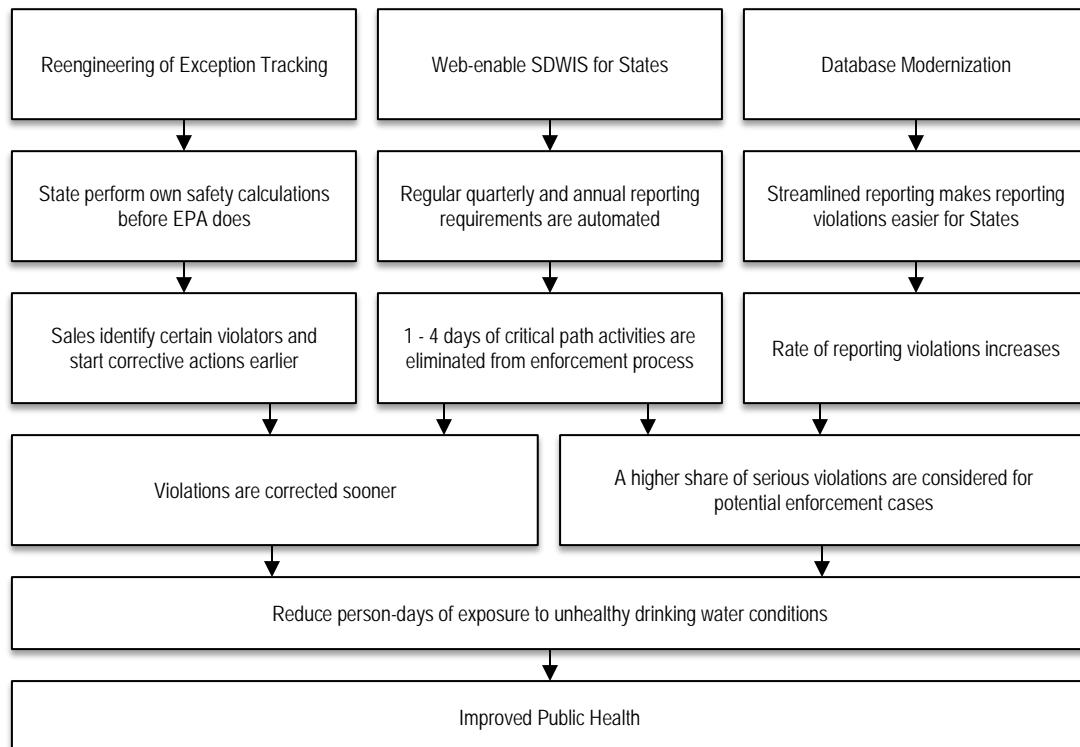
Step 1: Project Preparation

The group identified 12 persons that could represent the expertise of the EPA on SDWIS and its value. They also scheduled five half-day workshops to take place within a three-week period.

Step 2: Decision Model

During the first workshop, they realized that they were not concerned about SDWIS as a whole, but that the real dilemma was about the justification of three specific improvements to the SDWIS:

1. Reengineering an exception tracking system
2. Web-enabling the application for access by states
3. Modernizing the database



These three initiatives required initiation commitments of \$1 million, \$2 million, and \$500,000, respectively, plus ongoing maintenance. Each of these improvements also require three separate business cases displayed in the previous figure.

Step 3: Preliminary Measurements

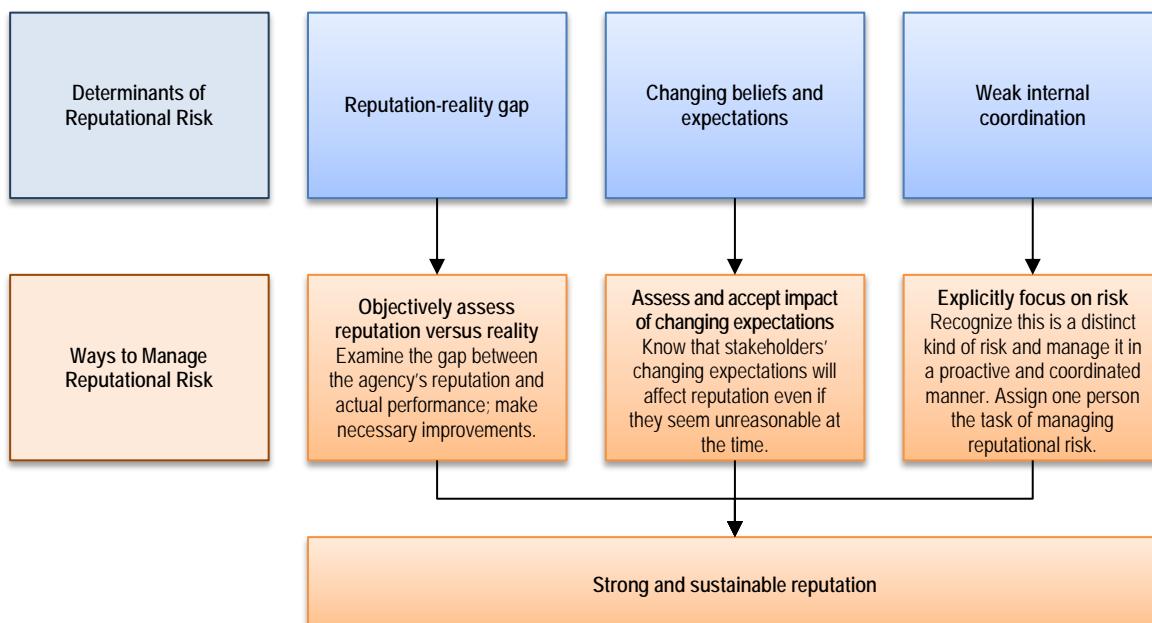
In Step 3, the group ran a VIA. Even though the ranges in all the variables expressed a lot of uncertainty, only one variable merited measurement: the average health effects of new save drinking water policies. While the upper bound of potential health benefits for any single policy was on the order of \$1 billion per year, there was also a chance of the benefit could be lower than the cost of compliance for the policy. In other words, the economic benefits of these policies were so uncertain that they actually allowed for the possibility that the net benefits were negative.

Step 4: Metrics Design and Final Deliverable

Finally, the group ran a final Monte Carlo simulation on each of the three investments. With the reduced uncertainty about the economic benefits of the water policies, each one turned out to be highly desirable investments. The improved exception reporting had a very high potential return, but there was enough uncertainty that there was still a 12% chance of a negative return. There was also a need for some ongoing metrics. Adoption rates by state users and how quickly the new system could be implemented were two of the more uncertain items. The consulting group working with the EPA and recommended that they accelerate the other two investments and defer the reengineering of exception reporting.

N.3. REPUTATIONAL RISK FRAMEWORK

The following was provided by the Harvard Business Review Magazine in the February 2007 edition.⁵⁶



⁵⁶ Eccles R., Newquist S., and Schatz R. (2007). "Reputation and its Risks." Harvard Business Review. February 2007. <<https://hbr.org/2007/02/reputation-and-its-risks>>.

This page is intentionally blank.

APPENDIX O. PRELIMINARY HAZARD ANALYSIS

What is it? Preliminary Hazard Analysis (PHA) is a semi-quantitative analysis that is implemented in the earliest stages of system design. The purpose of this analysis is to identify any potential hazards or accidental events that may be created by the system. PHA also requires that all of the hazards identified go through a severity ranking process which is followed by steps to formulate the appropriate measures to deal with these hazards.

Some of the following items that the Preliminary Hazard Analysis considers prior to the development of the system include:

- Hazardous components
- Safety related interfaces between various system elements, including software
- Environmental constraints including operating environments
- Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures
- Facilities, real property installed equipment, support equipment, and training
- Safety related equipment, safeguards, and possible alternate approaches
- Malfunctions to the system, subsystems, or software

Why use it? **Helps ensure that the system is safe** - When beginning a new and potentially hazardous system development project it is important to know the risks involved with carrying out each stage. PHA provides the stakeholders of the project with an indication of the risk, their severity, and the point within the development life-cycle that these risks should be considered.

More cost effective - Modifications are less expensive and easier to implement in the earlier stages of design. If a system experiences an unknown hazard it is more likely to cause greater monetary damage than if it were identified and prevented prior to its implementation.

Decreases design time by reducing the number of surprises - In many projects, scope creep and project surprises are one of the most common causes for a project to run over on both time and budget.

Timing Enhance Phase: PHA should be applied during the early phases of all new system development projects that have the potential to create conditions that may result in a hazardous event.

Steps The PHA methodology is comprised of the following five steps:

1. Identify known hazards.
2. Determine the cause(s) of the hazards.
3. Determine the effects of the hazards.
4. Determine the probability that an accident will be caused by a hazard.
5. Establish initial design and procedural requirements to eliminate or control hazards.

- Tips**
- **Hazards must be foreseen by the analysts** - Typically after an analysis has been completed, the decision makers and people involved tend to think that they have identified all the hazards that could negatively impact the system under analysis.
 - **The effects of interactions between hazards are not easily recognized** - While some of the effects of these hazards have been experienced in the past, sometimes the effects of a hazard are not as easily predicted. It is important to remember that the analysts reviewing this system are not omnipotent and there may be flaws in some of the results.

0.1. PHA STEPS

Step 1: Identify known hazards.

The first step of this methodology is to research the potential hazards that are already known to the members of the project team. This will launch the team into thinking about the potential hazards that are not known to them. This process can begin by breaking the analysis into four high-level categories, which include:

1. Known Potential Areas for Failure
2. Known Hazard Groups
3. Unknown Potential Areas for Failure
4. Unknown Hazards

Tip: Identifying the areas of failure and hazard groups can be done by consulting subject-matter experts (SMEs) or by researching hazardous events that have happened in the past. Unless you are venturing on the creation or analysis of an entirely unknown system, this information should be available for collection.

Part One (1-1): Build a Hazard Matrix

Preliminary Hazard Matrix						
System/Operation:						
Evaluator:						
Date:						
Hazard Group	Potential Areas for Failure					
	Structural	Electrical	Pressure	Leakage/Spill	Mechanical	Procedural
Collision/Mechanical Damage						
Loss of Habitable Atmosphere						
Corrosion						
Contamination						
Electric Shock						
Fire						
Pathological						
Psychological						
Temperature extremes						
Radiation						
Explosion						

An efficient way to organize these categories is in a Hazard Matrix. The figure above is a Hazard Matrix that has been altered from its original version by The Department of Mechanical Engineering at the University of Utah.^{57, 58} You should change the Potential Areas for Failure and Hazard Groups found in the example diagram and template to meet the criteria for the system being analyzed.

Part Two (1-2): Complete the Hazard Matrix with KNOWN information. Once you have collected a detailed history of the hazardous events that threaten your system through research and the consultation of a SME, you should fill in the template found above with this information.

Part Three (1-3): Complete the Hazard Matrix with UNKNOWN information. To identify new hazards and areas of the system that require attention you should conduct additional research applying other structured analytic techniques such as:

- Divergent-Convergent Thinking ([Appendix C.3](#))
- Hazard and Operability Analysis ([Appendix K](#))

Once you have collected all of the information you need on the unknown hazards and areas of concern and included them in your Hazard Matrix you can move on to Step 2.

Step 2: Determine the cause(s) of the hazards.

In this step of the analysis, you will identify the cause of the hazards that have been identified as a concern in Step 1. This can be done by conducting either Cause and Effect Analysis ([Appendix C](#)) or Root Cause Analysis ([Appendix S](#)); both of these techniques can provide the origins of these hazards.

Step 3: Determine the effects of the hazards.

Similar to step 2 you can identify the potential consequences in these hazards coming to fruition by completing the Cause and Effect Analysis which is an analytic technique that uses a diagramming tool called the fishbone or Ishikawa Diagram.

Step 4: Determine the probability that an accident will be caused by a hazard.

Determining the probability of an accident occurring can be done in two ways, either by conducting a preferred type of quantitative risk analysis of your choosing, or by a process of estimating the occurrence rating. The occurrence rating, or OCC, answers the following question: *What is the likeliness that the particular failure mode caused by the particular failure mechanism will occur?*

⁵⁷ Preliminary Hazard Analysis Packet. The Department of Mechanical Engineering: University of Utah. <http://www.mech.utah.edu/ergo/pages/Educational/safety_modules/Pha/PHA_ns.pdf>

⁵⁸ Vincoli, Jeffrey W. *Basic Guide to System Safety*. New York: Van Nostrand Reinhold, 1993. Print.

OCC is typically rated on an ordinal scale from 1 to 10, where 1 is extremely unlikely and 10 is inevitable or guaranteed. Values of 0 for Occurrence may also be included. Alternative scales may be used for Occurrence, including quantitative scales (interval, ratio and logarithmic scales), non-numeric ordinal scales, and scales based on uncertainty measures (e.g., probability). A sample table of Occurrence Levels is shown below:

Rating	Description	Definition
10	Very high	Tailor the labels and definitions to meet your specific needs. <i>Tip: It often helps to define a timeframe for which to evaluate the occurrence likeliness for each postulated root cause.</i>
9	High	
8	High	
7	High	
6	Moderately High	
5	Moderate	
4	Moderately Low	
3	Low	
2	Low	
1	Remote	

Step 5: Establish initial design and procedural requirements to eliminate or control hazards.

Similar to identifying the hazards that require attention, identifying the fixes and solutions to these hazards can be found the same way. There are a number of structured analytic techniques that can be used, to include:

- Premortem Analysis ([Appendix P](#))
- Divergent-Convergent Thinking ([Appendix C.3](#))
- Hazard and Operability Analysis ([Appendix K](#))

This page is intentionally blank.

APPENDIX P. PREMORTEM ANALYSIS

What is it? Premortem Analysis allows a group of analysts or stakeholders (i.e., team) to examine the various factors that could inhibit the success of a plan. The purpose of a Premortem Analysis is to find key vulnerabilities within a plan in order to find ways to improve its success.⁵⁹ By beginning the exercise with a hypothetical future (i.e., the plan has failed) and exploring the various factors that led to this future, the team can identify potential problems with the plan. Identifying these factors that could lead to failure helps the team discuss changes that could be made to avoid some of these potential problems.

- Why use it?**
- Premortem Analysis enables the team to describe weaknesses in a plan that have not been uncovered or mentioned by any members of the group. It gives the participants an opportunity to critique both their own ideas and others' ideas in an open environment. Because people are often reluctant to criticize their own ideas or plans, this places an emphasis on improving the plan by examining potential problems in the plan.
 - By examining these potential problems at the beginning stages of the plan, it sensitizes and trains the team to pick up on early warning signs that a plan may not work as expected. The participants can then learn how to question plans as they are being made and to identify weaknesses along the way.
 - Premortem Analysis also allows time-constrained teams to quickly test the underlying assumptions in their plan.
-

Timing Assess and Enhance Phases: Premortem Analysis works best when it is implemented at the beginning of the planning process. This allows the team to evaluate the potential problems with its current plan at its earliest stages. By implementing this early in the planning process, it sensitizes the team members to the current assumptions they have regarding the success of the plan and trains them to recognize these assumptions during the rest of the planning process.

Steps The following method for Premortem Analysis was taken from the book entitled *The Power of Intuition: How to Use Your Gut Feelings to Make Better Decisions at Work*. The Premortem Analysis consists of the following six steps:

1. Describe the plan.
2. Imagine how the plan could fail.
3. Brainstorm reasons why the plan failed in this manner.

⁵⁹ Klein, Gary A. *The Power of Intuition: How to Use Your Gut Feelings to Make Better Decisions at Work*. New York: Currency/Doubleday, 2003. Print.

4. Consolidate individual lists into a master list of failure modes.
 5. Revisit the plan and revise as appropriate.
 6. Periodically review the list through execution of the revised plan.
-

Tips If a team finds few or no factors for failure after the process is complete, it could lead to a false sense of security in the plan. These results could lead a team to believe its plan is invulnerable. Instead of training members to identify vulnerabilities in a plan, this could give them more confidence in their original plans, and keep them from critiquing their plans and ideas.

The use of Premortem Analysis could turn a team from being overly optimistic about its plan to being overly pessimistic about its plans. The team should be cautious of too quickly identifying flaws in the plan.

As with most analytic tools and techniques, the outcomes from a premortem exercise are only as good as the people chosen to participate. Ensure that all participants are well versed in the problem, and preferably are subject-matter experts.

P.1. PREMORTEM ANALYSIS STEPS

Step 1: Describe the plan. Gather a group of participants for the Premortem Analysis. This could include members from the team that created the plan or people from outside the team that had created the plan. It may be more helpful to have others that do not have any attachment to ideas within the plan participate because they may be a less bias participant.

To avoid confusion for those working on the plan and/or to familiarize other participants with the plan, the leader or other designee should describe the current plan in detail.

Step 2: Imagine how the plan could fail. The team leader tells the group that their plan has failed without mentioning or suggesting any reasons why. The leader can also describe the effects the failure of the plan had – both on the current group or a larger context.

Step 3: Brainstorm reasons why the planned failed in this manner. The leader asks each member to independently write down any possible reason the plan has failed on their own piece of paper. The leader should emphasize the need to criticize the plan in order to improve its success.

Step 4: Consolidate individual lists into a master list of failure modes. The leader should call on each member to share one factor from his/her list at a time (see the article on Round-Robin Brainstorming, [C.5](#)). This should be repeated until each member has shared all of their factors of failure. Discussion of these factors should be saved for later in the process. When first consolidating the individual list, the goal is to record each possible factor for failure on the master list.

NOTE: Participants should be encouraged to add new ideas brought about from hearing others mention theirs.

Step 5: Revisit the plan and revise as appropriate. The team should revisit the plan and address some of the factors mentioned that could potentially inhibit its success. Members should discuss ways to improve the factors of failure or ways to avoid the potential problems that are included on the master list. The discussion may evolve in such a way that there is a need to add more factors to the list.

It may be helpful here to systematically score or classify each factor on the basis of its perceived importance using Weighted Ranking ([Appendix X](#)). In addition, one could proceed with a vote on which factors should stay or be removed using a voting technique.

The factors obtained from a Premortem Analysis may be used to create a plan-specific, factor based model for assessing the risk of plan failure.

Step 6: Periodically review the list through execution of the revised plan. The team should periodically review the master (or modified) list as it continues to expand, and execute the revised plan. There are several different ways to keep the possibility of failure fresh in the team's mind.

The following include a few ways to review the list.

- Bring the list to each meeting and keep it on hand as the plan continues to develop. Feel free to discuss the relevance and completeness of the factors again at each meeting.
- If Premortem is performed at the beginning stages, when the plan is further developed make the list the center of the next meeting to view how the plan has improved and what areas are still potential problems.
- Remind each individual to independently review the list before meetings so that the members become accustom to picking up on flaws in the plan.

NOTE: The quantification of a risk analysis may not be useful in scrubbing a plan or decision option, and the team may be better served by appreciating the limitations of the plan or decision option.

P.2. ILLUSTRATIVE EXAMPLE

The following case study applies Premortem Analysis technique to understand possible causes for failure in the emergency communications plan for Centre County's Amateur Radio Emergency Service (ARES)/Radio Amateur Civil Emergency Service (RACES) network. For the purposes of this exercise, the following scenario was presumed to have occurred: *Communications were unable to be established between a care center and the Red Cross.*

Step 1: Describe the plan. The group first decided on a scenario for discussion. For this exercise, the group decided to state that the plan was to establish a radio link between an aid station in State College and the Red Cross. The plan was outlined in planning documents, as it was already in place and operational. The ARES members simply reviewed their protocols and the broad strokes of the plan before continuing on to the next step.

Step 2: Imagine how the plan could fail. Here the group imagined failure to be the case where the ARES/RACES network was unable to establish communications between a care center and the Red Cross.

Step 3: Brainstorm reasons why the planned failed in this manner. The leader of the exercise announced that the plan had failed, and instructed each ARES operator to generate their own list of possible causes for failure. The following lists were generated:

ARES Operator #1

- Politics
- Lack of understanding
- Rodents eating the equipment
- Equipment inaccessible

ARES Operator #3

- Incorrect frequency
- Lack of power
- No internet access in the field
- Rodents eating the equipment
- Immediate risks to personal safety of my family
- Political disputes
- Frequencies jammed

ARES Operator #2

- Lack of power
- Personnel untrained
- Frequencies jammed
- Equipment malfunctions
- Lack of pre-agreed frequencies
- Radios not powerful enough
- Equipment inaccessible
- Politics prevent communication

Interested Citizen

- Equipment inaccessible
- Lack of understanding
- Equipment failure
- Lack of power
- Lack of repeaters or infrastructure
- Not enough people to run the network
- Frequencies jammed
- No spare parts to repair radios
- Operators freaking out
- “Pile-up,” too many operators talking at once

Step 4: Consolidate individual lists into a master list of failure modes. One by one, each participant read off a single unique reason in turn. Each suggestion was written on a whiteboard to form a master list for all to see and consider.

Step 5: Revisit the plan and revise as appropriate. After generating the list of possible causes, each possible cause was discussed, and each participant was asked to list their top 3 concerning causes. The following list is a ranked reproduction of that list, most concerning on top.

1. Lack of understanding of what is going on
2. Inaccessible or improperly stored equipment
3. Lack of personnel
4. Incorrect frequencies used / improperly trained operators
5. Insufficient or unavailable power
6. Interpersonal conflict

Step 6: Periodically review the list through execution of the revised plan. The participants decided that this exercise was an extremely useful tool in determining how to improve the emergency communications plan. A document was drawn up showing the concerns and their ranking, and a follow-up meeting was planned exactly 6 months from the original exercise to repeat the process and see if any of the changes they implemented were effective.

This page is intentionally blank.

APPENDIX Q. PROBLEM RESTATEMENT AND ISSUE DEVELOPMENT

What is it? Problem Restatement and Issue Development is a technique used to ensure that the central issues and alternative explanations of an issue or problem are identified within the scope and focus of the problem statement.^{60, 61} This technique helps analysts and decision makers develop and articulate the most significant questions underlying their analytic or decision tasks.

Why use it? The Problem Restatement and Issue Development technique can save a great deal of the time and effort that is easily misspent on research and analysis of poorly stated questions or decision problems that gives free rein to the analyst's bias. Poorly stated issues frequently fall into the following categories:

- Issue is solution driven (Where is the WMD in Iraq?)
- Issue is assumption driven (When China launches rockets into Taiwan, will the Taiwanese government collapse?)
- Issue definition is too broad or ambiguous (What is the status of Russia's air defenses?)
- Issue definition is too narrow or misdirected (Who is voting for Party A in the election?)

Timing Problem Restatement and Issue Development should be used anytime an analyst or decision maker begins to assess a new issue or problem or begins a new research endeavor to mitigate bias toward the issue. This technique may be used at any point throughout the analytic process. It is especially useful when a new hypothesis, key risk question, decision task or new data is introduced. This method is also helpful when reexamining the premises or basis of a key risk question or problem when an individual is "stuck" on how to proceed.

Steps The Problem Restatement and Issue Development technique consists of the following three steps:

1. Articulate the original question
2. Explore variations of the original question
3. Settle on a final revised question and describe its nuances

⁶⁰ *A Tradecraft Primer: Basic Structured Analytic Techniques*. Defense Intelligence Agency. March 2008, pp. 6-7.

⁶¹ Jones, Morgan D. *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving*. New York: Three Rivers, 1998. Print.

Tips

- Although issue identification only takes 5 to 10 minutes with practice, analysts new to the technique tend to think it takes too long to accomplish. Poorly articulated issues, questions, or tasks are more difficult to redefine and may require reengaging with the source of the issue for clarification.
- If time permits, pass the original and final questions to others for peer-review. Encourage them to also apply the Problem Restatement and Issue Development technique.

Q.1. PROBLEM RESTATEMENT AND ISSUE DEVELOPMENT STEPS

Step 1: Articulate the original question

In this step, write down the original key risk question. If using a whiteboard in a group setting, write this question in big letters for everyone to see. Do not spend any time trying to revise the original question. Refer to the original question throughout steps 2 and 3.

Step 2: Explore variations of the original question

Provided below are six strategies designed to help analysts and decision makers properly identify the most significant problem statement or issue. The following processes may be used in any order and should be used together to identify the central issues and alternative ways of stating them.

1. Paraphrase the original question
2. Flip the original question 180-Degrees
3. Broaden the Focus of the original question
4. Narrow the Focus of the original question
5. Redirect the Focus of the original question
6. Ask “Why” of the original question

Each of these six strategies is described below. Note that these strategies are not all encompassing, but rather represent only a small number of ways of exploring alternative questions.

Paraphrase the original question

Redefine the issue without losing the original meaning. Review the results to see if they provide a better foundation upon which to conduct the research and assessment to gain the best answer. Example: the original question, “How much of a role does Aung Sung Sui Kyi play in the ongoing unrest in Burma?” is rephrased as, “How active is the NLD headed by Aung Sung Sui Kyi in the current antigovernment riots in Burma?”

Flip the original question 180-Degrees

Turn the issue on its head. Is the issue the one asked or the opposite of it? Example: the original question, “How much of the PLA ground capability would be involved in an initial assault on Taiwan?” is rephrased as, “How much of the PLA ground capability would NOT be involved in the initial Taiwan assault?”

Broaden the Focus of the original question

Instead of focusing on only one piece of the puzzle, step back and look at several pieces together. What is the issue before you connected to? Example: the original question, “How corrupt is President Musharraf?” leads to the question, “How corrupt is the Pakistani government?”

Narrow the Focus of the original question

Can the issue be broken down further? Take the question and ask about the components that make up the problem. Example: the original question, “Will the EU ratify a new constitution?” can be broken down to, “How do individual member states view the new EU constitution?”

Redirect the Focus of the original question

What outside forces impinge on this issue? Is deception involved? Example: the original question, “What are the terrorist threats against the U.S. homeland?” is revised to, “What opportunities are there to interdict terrorist plans?”

Ask “Why” of the original question

Ask “why” of the initial issue or question. Develop a new question based on the answer. Then ask “why” of the second question and develop new question based on that answer. Repeat this process until you believe the real problem emerges. This process is especially effective in generating possible alternative answers.

Step 3: Settle on a final revised question and describe its nuances

Based on the insights generated through careful reexamination of the original question, this last step settles on the most significant question that gets to the heart of the issue under study. Provide a short summary of the nuances underlying this revised question.

Q.2. ILLUSTRATIVE EXAMPLES

The following demonstrates how the use of the Problem Restatement and Issue Development technique can be used to go from a general key risk question of interest to one that gets to the heart of the matter. The focus of this example is on pandemic preparedness in a region.

Step 1: Articulate the original question

The original question is as follows: *Is the region prepared to provide treatment to thousands of sick persons in the event of a pandemic?*

Step 2: Explore variations of the original question

A single analyst reconsidered the original question using each of the six strategies comprising the Problem Restatement and Issue Development technique. A summary is provided below.

Paraphrase the original question

Does the region have the capability to treat thousands of sick persons in the event of a pandemic? This revised question makes a slight adjustment to the wording of original question.

Flip the original question 180-Degrees

Is the region unprepared to provide treatment to thousands of sick persons in the event of a pandemic? This revised question considers whether the region is unprepared versus being prepared.

Broaden the Focus of the original question

What is the maximum capacity of the region to treat sick persons at any given time? Rather than consider whether the region is prepared or not, this revised question examines the broader issue of capacity to treat sick persons.

Narrow the Focus of the original question

What specific capabilities does the region have to treat sick persons in the event of a pandemic? This question looks more closely at the specific capabilities to treat sick persons in the region versus the broader question of whether the overall capabilities are enough to deal with a potential pandemic.

Redirect the Focus of the original question

How could the flu escalate into a pandemic in the region? This revised question redirects the focus on how the flu could escalate into a pandemic instead of whether the region is prepared in the event one should occur.

Ask “Why” of the original question

The following follows a sequence of asking why. For each response to the question, we again ask why until we get to the heart of the issue.

- Why would the region be able or unable to adequately treat thousands of sick persons in the event of a pandemic? Because many of the doctors and nurses would also be sick and due to a shortage of needed medicine.
- Why would the doctors and nurses be sick? Because they did not get vaccinated.
- Why did they not get vaccinated? Because vaccination was not compulsory and the region did not provide any incentive for potential recipients.
- Why would there be a shortage of medicine? Because they were used for other purposes.
- Why were they used for other purposes? Because the region did not enforce rationing.
- Why would a pandemic occur in the region? Because the public did not take the matter seriously.
- Why did the public not take the matter seriously? Because guidance on preventing illness was not distributed.

Step 3: Settle on a final revised question and describe its nuances

Based on the insights generated through systematic reconsideration of the original question, the analyst produced the following revised question:

What guidance on prevention could the region offer to the public in attempt to minimize the chances of a pandemic AND what can be done to ensure availability of medical practitioners and medicine in the event one should occur?

Note that in this example we went from a single general question to two specific questions that relate to the significant issues. The following key points were provided as justification for this revised question:

- Medicine is scarce
- Medical practitioners are necessary for administering medicine
- There are far fewer practitioners relative to the size of the exposed population
- The public is not as informed as it could be
- “Knowing is half the battle”

This page is intentionally blank.

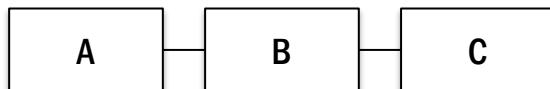
APPENDIX R. RELIABILITY BLOCK DIAGRAMS

Reliability Block Diagrams (RBDs) are graphical illustrations of how the failures of system components interact to cause the failure of the entire system. An RBD expresses the paths a system need to take to reach a successful end state. The block diagram is similar to a Fault Tree Analysis (FTA) diagram ([Appendix J](#)), the fundamental difference being that an RBD works within the “success space” of a system where the FTA works within the “failure space” of a system.⁶²

The way in which an RBD expresses the system being studied is through the logical connection working system components. Moving from left to right there are one to several paths that are conditions for the successful operation of a system. Large systems containing many parts are typically formed by using a combination of two basic configurations.

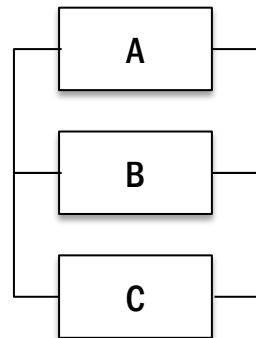
R.1. SERIES SYSTEM

A system whose components are in series requires all components to work to ensure system success. Consequently, failure of any single component results in failure of the overall system. In a series system, any particular failure mode leading to component failure is known as a single point failure. An RBD depicting a simple system comprised of 3 components (labeled “A”, “B” and “C”) connected in series is shown below.



R.2. PARALLEL SYSTEM

A system whose components are in parallel requires only one component to work to ensure system success. Consequently, all components within the system must fail to result in failure of the overall system. Components within a simple parallel system are said to be redundant. An RBD depicting a simple system comprised of 3 components (labeled “A”, “B” and “C”) connected in parallel is shown.



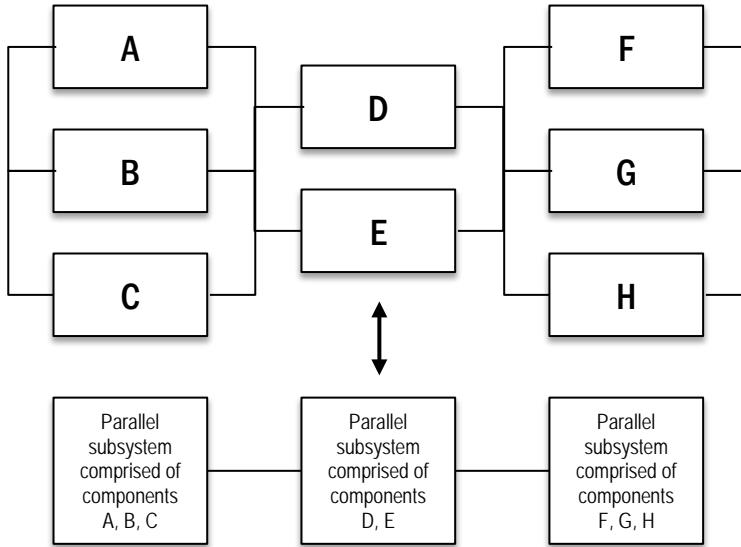
R.3. SPECIAL CASES

A number of more complicated systems can be defined that consist of some components arranged in series and others arranged parallel. Special cases of mixed systems include series-parallel systems (a series of subsystems with components in parallel) and parallel-series systems (parallel subsystems with components in series).

⁶² “Comparing Fault Trees and RBDs.” Weibull. <http://www.weibull.com/SystemRelWeb/comparing_fault_trees_and_rbds.htm>.

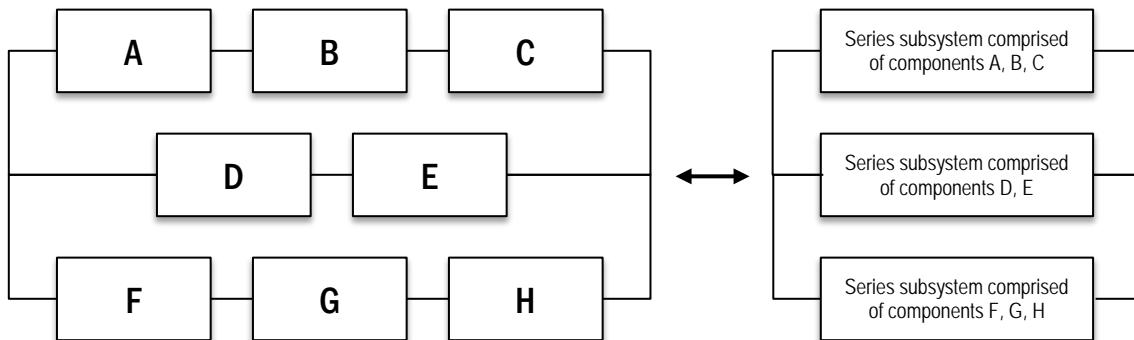
R.3.1. Series-Parallel System

A series system of subsystems comprised of components arranged in parallel is known as a series-parallel system. An RBD depicting a series-parallel system comprised of eight components (labeled A-H) is shown below.



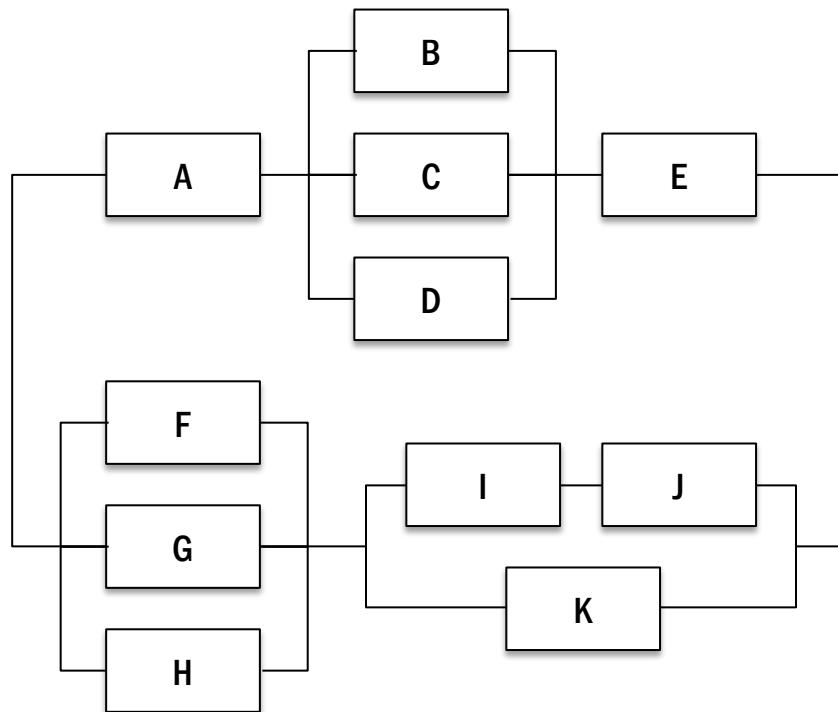
R.3.2. Parallel-Series System

A parallel system of subsystems comprised of components arranged in series is known as a parallel-series system. An RBD depicting a parallel-series system comprised of eight components (labeled A-H) is shown below.



R.3.3. General Mixed System

A system comprised of any combination of series and parallel subsystems, sub-subsystems, etc. is known as a general mixed system. A RBD depicting a series-parallel system comprised of eleven components (labeled A-K) is shown below. Both series-parallel and parallel-series systems are special cases of a general mixed system.



This page is intentionally blank.

APPENDIX S. ROOT CAUSE ANALYSIS

What is it? Root Cause Analysis is a systematic approach that seeks to identify the origin of a problem. Using a detailed list of steps and creating a Fishbone diagram to help analyze the situation to find the primary cause of the event. It is a belief in a Root Cause Analysis that a system and the events that occur are interrelated. Using this methodology, it is possible to trace back the actions that have taken place and by doing this discover where the problem has originated.⁶³

*Root Cause Analysis is the fundamental breakdown or failure of a process which, when resolved, prevents a recurrence of the problem.*⁶⁴

In a Root Cause Analysis there are three basic categories of causes, which include:

1. Physical causes - Tangible, material items failed in some way (e.g., a car's brakes stopped working).
2. Human causes - People did something wrong, or did not do something that was needed. Human causes typically lead to physical causes (e.g., no one filled the brake fluid, which led to the brakes failing).
3. Organizational causes - A system, process, or policy that people use to make decisions or do their work is faulty (e.g., no one person was responsible for vehicle maintenance, and everyone assumed someone else had filled the brake fluid).

Why use it? In the Assess Phase, a Root Cause Analysis can be used for the following purposes:

- To determine what happened.
- To determine why it happened.
- To figure out what to do to reduce the likelihood that it will happen again.

Timing Root Cause Analysis can be used when there is a need to break down a problem in order to determine the cause.

Steps Root Cause Analysis is comprised of the following five steps:

1. Define the problem
2. Collect data
3. Identify possible causal factors
4. Identify the root cause(s)
5. Recommend and implement solutions

⁶³ "Root Cause Analysis." Mind Tools. <http://www.mindtools.com/pages/article/newTMC_80.htm>.

⁶⁴ "Root Cause Analysis." NASA. <<http://process.nasa.gov/documents/RootCauseAnalysis.pdf>>

- Tips**
- Figure out what negative events are occurring. Then, look at the complex systems around those problems, and identify key points of failure. Finally, determine solutions to address those key points, or root causes.
 - It's okay to start by performing Root Cause Analysis on large problems so that you can discover the tie between unresolved small problems and large problems. But only doing Root Cause Analysis on big problems will assure that you will continue to have big problems. Eventually, you need to do Root Cause Analysis on your unresolved small problems.⁶⁵
 - A similar technique that may help in discovering the root cause of a problem is the Cause and Effect Analysis ([Appendix C](#)).
 - This is an iterative process that may require several redundant steps that require several Fishbone Diagrams to reach the final root cause of the problem.
 - Seeking the “root cause” is an endless exercise because no matter how deep you go there’s always at least one more cause you can look for.⁶⁶

S.1. ROOT CAUSE ANALYSIS STEPS

Step 1: Define the Problem

It is important to clearly describe the specific problem that is under analysis. A good starting point is to begin answering the following questions:

- What do you see happening?
- What can you hear?
- What are the specific symptoms?

Step 2: Collect Data

Data collection is necessary to begin dissecting the problem being analyzed and to find its root cause. Typically if a problem exists there is evidence that has been left behind to learn from.

Again some questions to ask include:

- What proof do you have that the problem exists?
- How long has the problem existed?
- What is the impact of the problem?
- What can we rule out?

Tip: It is suggested that if an analyst cannot collect the necessary information of the problem, than it would be beneficial to consult an expert to gather the data needed.

⁶⁵ Nelms, Bob. “Root Cause Analysis.” Failsafe Network, Inc. <<http://www.failsafe-network.com/>>.

⁶⁶ Bellinger, Gene. “Root Cause Analysis.” Systems Thinking. <<http://www.systems-thinking.org/rca/rootca.htm>>.

Step 3: Identify Possible Causal Factors

In step 3 it is good to begin to identify possible causal factors by taking a top-down approach.

There are typically six primary categories that can be used to identify the cause of an event.⁶⁷

These categories include:

1. People: Anyone involved with the process.
2. Methods: How the process is performed and the specific requirements for doing it, such as policies, procedures, rules, regulations, and laws.
3. Machines: Any equipment, computers, tools, etc. required to accomplish the job.
4. Materials: Raw materials, parts, pens, paper, etc. used to produce the final product.
5. Measurements: Data generated from the process that are used to evaluate its quality.
6. Environment: The conditions, such as location, time, temperature, and culture in which the process operates.

Part One (3-1): Incorporate primary categories into a Fishbone Diagram. One method that has been used to systematically break down a problem is by using a Fishbone Diagram. You can start your analysis by incorporating the six primary categories into the diagram.

Part Two (3-2): Identify which of the primary categories caused the problem under analysis.

Pinpointing the category that caused the problem in question is a significant step forward, because you can then identify the specific factors that contribute to the problem.

Part Two (3-2): Identify what events, or failure, could contribute to the problem under analysis. If analyzing the machinery shown in the example above, you should ask what events could result in the failure of machinery.

If you identify an answer to this question, ask again if the solution to that question also has possible causes. For example:

- Why did I fall off my bike?
 - I was going too fast.
 - Why were you going so fast?
 - The brakes where loose.

Step 4: State the Root Cause(s)

Once you have identified the solution, the cause for an event occurring, you can state the root cause.

⁶⁷ Hankins, Judy. *Infusion Therapy in Clinical Practice*. St. Louis: Saunders, 2001. Print.

Step 5: Recommend and Implement Solutions

Finally, the last step of this process is to recommend and implement a solution. Once you have identified solutions to fix the root cause, it is important to identify other causes that may result in the same event. A popular method for identifying potential weaknesses in a system is the Failure Modes and Effects Analysis ([Appendix I](#)). By identifying potential failure modes you will be less likely to require a Root Cause Analysis on the same system in the future.

S.2. ILLUSTRATIVE EXAMPLE

In this illustrative example we identify the root cause of a car being pulled over on the side of the road.

Step 1: Define the Problem

The problem that exists is that a car is on the side of the road and the engine is smoking, hissing, and there is also engine fluid dripping from the underside of the vehicle.

Step 2: Collect Data

Some of the evidence we have identified are the following:

- The car has been pulled over on the side of the road.
- The engine is smoking.
- Car will not start.
- The engine is making a hissing noise.
- There is engine fluid leaking on the ground.
- The temperature is above 80 degrees.

Things to rule out:

- Gas tank was just filled.
- Oil is at an appropriate level.
- Car was not in an accident.
- Driver did not intend to turn the car off.

Step 3: Identify Possible Causal Factors

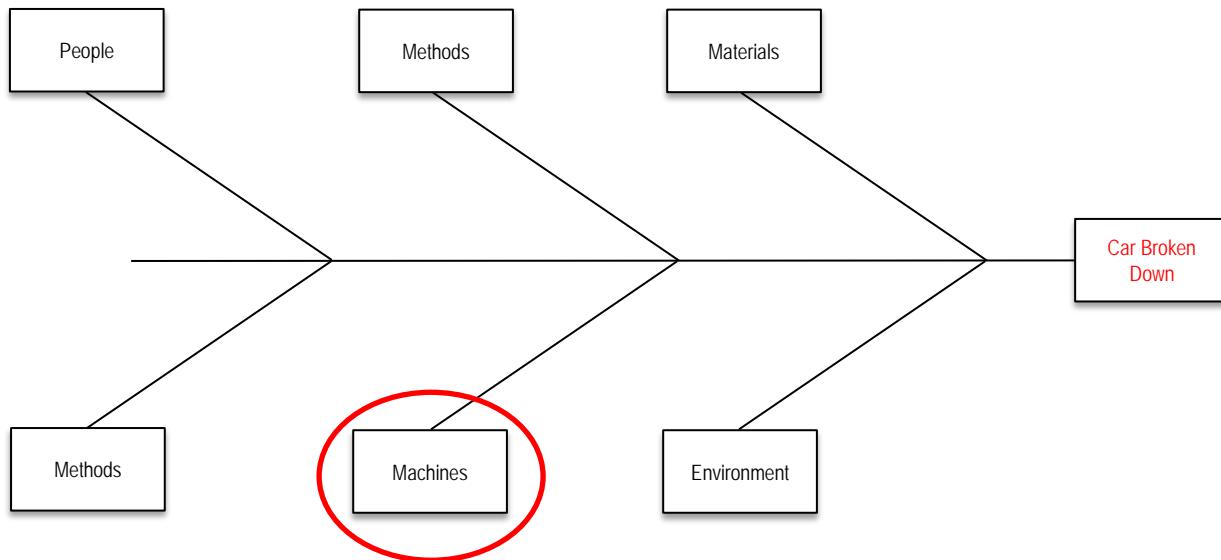
Causal Factors that are ruled out

1. People: We know the driver's intention was not to be pulled over on the side of the road.
2. Methods: The driver was following all of the policies, rules, procedures and regulations of the road.
3. Materials: The same materials were used in all of the other models of this vehicle and have passed the rigor of inspection.
4. Measurements: The data does not require any difficult analysis other than the use of visualizing the scene.

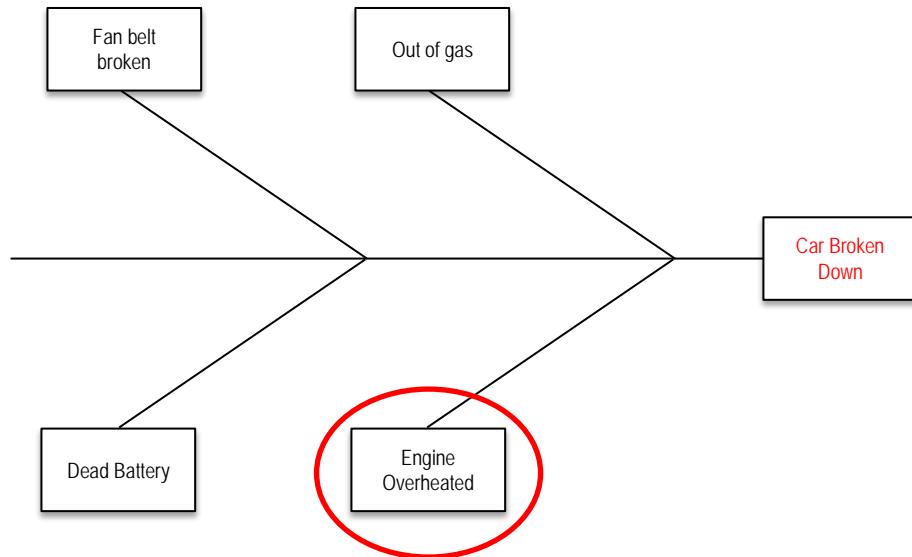
Potential Causal Factors

1. Environment: The temperature outside is above 80 degrees and could be the cause of the engine overheating.
2. Machines: The engine overheating could be a problem with mechanical problem. This means that some part of the engine system may be broken or have failed.

We have decided to rule out the environment as the root cause, because of the engine fluid leaking on the ground. While the environment could be a contributing factor we believe that the root cause is a mechanical issue.

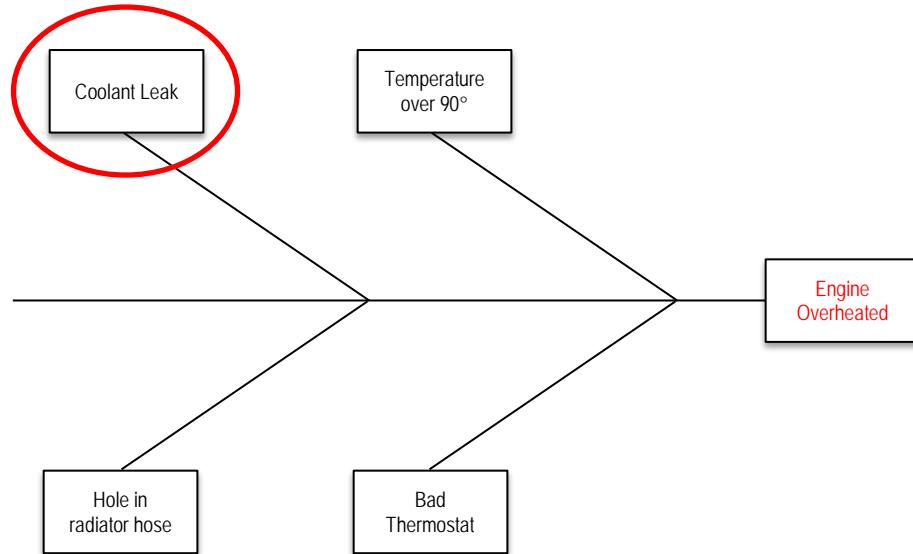


Part Two (3-2): Identify what events or failure could contribute to the problem under analysis. We have identified that the cause of the engine being on the side of the road is a mechanical failure. As shown below the car is on the side of the road because the car's engine has broken down. We display this on the following Fishbone Diagram.



Step 4: Identify the Root Cause(s)

The coolant that was found leaking on the ground tells us that the cause of the car being broken down on the side of the road is a coolant leak.



Step 5: Recommend and Implement Solutions

A solution to this problem is to repair the crack in the radiator. Another important solution to implement, which will prevent this from happening again, is to visit a mechanic regularly to ensure that your engine is functioning properly.

This page is intentionally blank.

APPENDIX T. SCOPING A RISK STUDY

What is it?	A process of defining the scope and boundaries of a project utilizing multiple methodologies.
Why use it?	A necessary element of a successful risk analysis activity is a clearly defined scope that sets the boundaries for analysis, definition of the system of interest and what about it is important, and the hazards that must be considered.
Timing	Develop Phase: When determining the scope of a risk study, several procedures need to be addressed. Always begin with defining the security context, which is represented by the interaction of the protector, assets, and threats in a given situation. This will lead to the identification of the key risk question and result in the analyst being able to define the system.
Steps	To specify the scope of a risk study, perform the following five steps. Step 1: Establish the security context by defining who the protector is, what he/she cares about (assets or values), what threats are of concern, and how they relate to one another. Step 2: Articulate the key risk questions that are of interest to the decision maker or necessary for him/her to complete the decision task. Step 3: Based on the security context and key risk questions of interest, proceed with developing a conceptual model of the corresponding system at a level of specificity (resolution) no greater or less than what is needed to support the analysis. Step 4: Identify the resources available to support analysis. Resources include time, number of analysts, skills of the analysts, and technological resources. Step 5: Use the Toolkit to select an ensemble of tools and techniques to help answer the key risk questions given available resources.

T.1. DEFINING THE SECURITY CONTEXT

What is it? Defining the Security Context specifies the bounds on what is considered and what is not considered in a risk study.⁶⁸ It does this by focusing on the main elements that bound the risk analysis within a particular situation.

- Protector. The protector defines the individual at the center of the risk analysis, defines what should be considered as a decision variable vice an input variable, defines the scope of risk considerations (e.g., which people, whose money, what else), etc.
- Assets. Identify the assets and values whose compromise might pose harm to the protector. Labeling of the assets enables one to proceed with Defining a System.
- Threats. The answer to this question (what are my threats?) constrains how different elements or “things” within the system can fail due to exposure to the hazards induced by the threat. That is, knowledge of the threats constrains the scope of vulnerability assessment on assets.
- Situation. The situation defines the environment or circumstances in which the protector, assets, and threats interact. The situation provides the background context for understanding how events unfold.

A security context is fully specified when the protector, assets, threats, and situation are defined. However, we note that the less specific any of these are, the more expansive the associated risk study must be to be complete.

Why use it? **Provides Scope.** A clearly defined security context provides the scope of a security risk study in terms of whose interests are at risk (Protectors), what those interests are (Assets), and what hazards are of concern (Threats).

- Knowing the Protectors allows one to establish the point of view for analysis, and in particular, how to assign value or importance to the compromise of an Asset.
- Knowing the Assets enables us to define a system and associated objectives; an item is an asset if its compromise can cause harm, loss or damage to the Protector.
- Knowing the Threats constrains the set of initiating events to only those within the scope of the associated capabilities and intentions to cause harm to the Protectors.

Identifies Comparable Risk Studies. Knowing the security context associated with two or more risk studies enables one to assess the extent to which the associated results are comparable. For example, any difference in the Protectors, Assets, or Threats between two or more studies enables one to draw comparisons.

⁶⁸ Manunta, Giovanni. *Defining Security*. Diogenes Paper. No. 1. Royal Military College of Sciences: Cranfield Security Centre, March 2000. <<http://www.srsi.org/diogenes.htm>>.

- For a fixed set of Assets and Threats, a difference in Protector enables one to compare ...
- For a fixed set of Protectors and Threats, a difference in Asset ...
- For a fixed set of Protectors and Assets ...

Timing	Defining a security context is a necessary prerequisite to commencing any security risk study. The concept of a security context can be extended to non-security related or all-hazard risk studies by substituting or expanding the definition of Threat to include natural phenomena or accidental conditions. However, the three elements no longer define a security context when non-security hazards are considered; rather, it may be more appropriately described as a safety context.
Steps	The method for specifying a security context consists of the following four steps: <ol style="list-style-type: none">1. Identify the protector2. Identify the assets3. Identify the threats4. Describe the situation, that which shapes the interactions of the protector, assets, and threats
Tips	<p>Defining the Protector, Asset, and Threat. In some situations the definition of the Protector, Asset, or Threat may overlap. For example, in the case of personal protection, the Protector and the Asset are the same entity. Similar examples can be conceived where the Protector is also the Threat, the Asset is also the Threat, and in the extreme where the Protector is the Threat and the Asset.</p> <p>In other situations, the details of the analysis may imply a security context without ever stating it explicitly. A broad definition of the Protectors, Assets, and Threats corresponds to broadly defined risk analysis effort. In the extreme, not specifying a security context widens the scope of the analysis to include any and all Protectors, Assets, and Threats under all conceivable circumstances. For example, a vaguely defined study that requires further qualification to be feasible is one that “assesses the risk of terrorism” without specifying from whose perspective and what interests are at stake. This infinitely wide scope poses an obviously intractable problem to analysts.</p> <p>Collectively Exhaustive Scope. A risk assessment will be assessed as incomplete unless it considers all possible interactions of Protectors, Assets, and Threats within its scope. Accordingly, completion of a widely-scoped risk study requires more resources due simply to combinatorial effects (e.g., ten assets from two different perspectives, subject to five different threats, results in 100 different individual Protector, Asset, and Threat combinations) and without even taking into account the level of specificity of the associated risk scenarios. Take care to specify the scope appropriately to meet the exact needs of decision making, no more or no less.</p>

T.1.1. Defining the Security Context Steps

Step 1: Identify the Protector

The protector defines the individual at the center of the risk analysis, defines what should be considered as a decision variable vice an input variable, defines the scope of risk considerations (e.g., which people, whose money, what else), etc.

Step 2: Identify the Assets

Identify the assets and values whose compromise might pose harm to the protector. The answer to this question enables one to proceed with a systems analysis.

Step 3: Identify the Threats

The answer to this question constrains how different elements or “things” within the system can fail due to exposure to the hazards induced by the threat. That is, knowledge of the threats constrains the scope of vulnerability assessment on assets.

Step 4: Describe the Situation

The situation defines the environment or circumstances in which the protector, assets, and threat interact. The situation provides the background context for understanding how events unfold. A security context is fully specified when provided with answers to the questions in steps 1-3. In general, the answer to step 4 is implied by the answers to the previous steps.

T.1.2. Illustrative Example

Consider the pictures below. One can identify a variety of security or safety contexts associated with these images. For the sake of illustration, we will articulate only one.

Example 1

- Who are the Protectors? Airport officials, passengers
- What are the Assets? Luggage
- What is the Threat? Passengers, Thief

Description: Any individual with the intent to steal luggage can easily get their hands on it.

Passengers can prevent this threat by reporting to the baggage claim as soon as they step off the

plane. More protection can be added by the airports. They should have security stationed around the baggage claim, but this form of protection is not always in place and it is impossible to know if someone is stealing a bag. The luggage can be stolen by another passenger, but it is more probable that it is stolen by someone who is not expecting to pick up their own luggage. A big vulnerability in this system is that anyone can walk into the section of the airport where the baggage claim is located.



Example 2

- Who are the Protectors? Police, Sober drivers
- What are the Assets? Safety of drivers on the road, condition of vehicle
- What is the Threat? Drunk driver

Description: All too often, people will have a couple of drinks and get behind the wheel. The logical protectors in this situation are police and other drivers. From their point of view, they are protecting the well-being of other drivers on the road as well as the condition of their vehicles. In this dangerous situation, a drunk driver can harm themselves, other drivers, and the vehicles in which they are situated.

**Example 3**

- Who are the Protectors? Local authorities, U.S. Nuclear Regulatory Commission, U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA)
- What are the Assets? Nuclear Power Plant
- What is the Threat? Terrorist, Employee

Description: Nuclear power plants are designed with an extremely high level of safety and security in mind. Local authorities and federal agencies prepare emergency response plans and have protocols in place to offset or mitigate any attack. People were always worried about the safety of nuclear power plants, but ever since 9/11, security against terrorist attacks has been fortified.



T.2. DEFINING A SYSTEM

What is it? Defining a System is a concept that builds upon the security context by identifying what systematically decomposing a system into assets will directly bear on the interests of the protector. Assets are defined as those objects whose performance bears on the different properties of the system in a manner that helps the system achieve its objectives.

Why use it? The goal, when Defining a System, is to develop a conceptual model of a system of interest defined in terms of its input, output, and state variables.

Timing Defining a System works well in conjunction with the SIPOC Diagram ([Appendix U](#)) to inform the Business Process Analysis.

Steps When Defining a System, the first objective is to name the system and establish the point of view (i.e., of the protector). If multiple points of view must be considered, the Hierarchical Holographic Modeling ([Appendix L](#)) technique may prove helpful.

For the points of view of interest, the next step is to articulate the success scenario by writing a statement of success and describing what constitutes failure. A success scenario is a concise statement of how a system must perform based on three dimensions:

- Capability (specifically, what is the system supposed to do?)
- Environment (under what conditions?)
- Duration (for how long?)

Throughout this process you will define output, input, and state variables to help formulate answers to the following.

In general, there are three variable types of interest with respect to a system. These are the input variables, output variables, and the internal or state variables. These variables are illustrated below.

Input variables are what go into the system. Input variables are of three types:

- Decision Variables: Inputs that are controllable by the decision maker (degrees of freedom)
- Environmental Variables: Inputs from the environment
- Exogenous Variables: Inputs coming in from outside the system boundary

Output variables define what comes out of the system. In the risk analysis context, output variables specify how well the system is performing. Accordingly, the values of the output variables can be used to determine whether the system is meeting the objectives for which it was designed. State variables (internal variables) describe what is going on in the system. These are variables that are typically modeled and used to estimate system performance. In general, input variables influence the state variables, and the state variables then interact to influence the output variables.

This page is intentionally blank.

APPENDIX U. SIPOC DIAGRAM

What is it? The Suppliers, Inputs, Processes, Outputs, Customers (SIPOC) Diagram defines the key elements, scope, and boundaries of a function.

Why use it? The SIPOC Diagram visually communicates a process at a high level by mapping the process to identify interdependencies, inputs, outputs, and the steps within the process. It is very useful in jump-starting the thought process in thinking in terms of cause and effect.

Timing Define Phase: The SIPOC Diagram is useful for modeling Business Process Analyses to inform and Business Impact Analyses. It supports the identification of the business process, requirements of the business process, interdependencies, and recovery requirements (e.g., resources).⁶⁹

Steps The SIPOC Diagram methodology is comprised of the following eight steps:

1. Create an area that will allow the team to post additions to the SIPOC Diagram. This could be a transparency (to be projected by an overhead) made of the provided template, flip charts with headings (S-I-P-O-C) written on each, or headings written on post-it notes posted to a wall.
2. Begin with the process. Map it in four to five high level steps.
3. Identify the outputs of this process.
4. Identify the customers that will receive the outputs of this process.
5. Identify the inputs required for the process to function properly.
6. Identify the suppliers of the inputs that are required by the process.
7. *Optional:* Identify the preliminary requirements of the customers. This will be verified during a later step of the Six Sigma measurement phase.
8. Discuss with project sponsor and other involved stakeholders for verification.

⁶⁹ Charantimath, Poornima M. *Total Quality Management*. Delhi: Pearson, 2011. pp. 406-07. Print.

U.1. SIPOC DIAGRAM VISUAL

Who is providing input into the function?	What are the inputs?		What are the start and end points of the function and the major steps in the process?		What are the outputs?		Who are the outputs being delivered to?
Suppliers	Input		Process (High Level)		Output		Customers
1	1		Start Point:		1		1
	2						2
	3				2		1
2	1		Operation or Activity		3		2
	2						1
	3		1				2
3	1		2		4		1
	2		3				2
	3		4		5		1
4	1		5		6		2
	2		6				1
	3		7				2
			8				
			9				
			10				
			11				
			End Point:				

This page is intentionally blank.

APPENDIX V. SORTING

What is it? Sorting is a basic structured analytic technique for grouping information to develop insight, identify patterns, uncover trends and spot anomalies.^{70, 71}

Why use it? Sorting massive amounts of data can provide insights into trends or abnormalities that warrant further analysis and that otherwise would go unnoticed. This technique can highlight new or additional analytic insights within an old intelligence problem or a new one. Sorting data before you begin analyzing transactions (e.g., COMINT or transfers of goods), is very helpful.

Timing Assess and Enhance Phases: Sorting is effective when information elements (e.g., factors from a factor-based model) can be broken out into categories or subcategories for comparison using an automated computer program such as a spreadsheet. This technique is most useful for reviewing massive set of information pertaining to the attributes of multiple assets, scenarios, etc.

Sorting also aids in the review of multiple categories of information (e.g., derived from a Data Classification System) that when broken down into components can present possible trends, similarities, differences, or other insights not readily identifiable. Sorting can be used at any stage and is particularly effective during initial data gathering and hypothesis generation.

Steps The Sorting technique requires that the analyst has, in hand, a database containing a particular information set of interest. In addition, this technique requires that the analyst is working with a fixed way of describing the data, such as a set of factors associated with a factor-based model or an ontology associated with a particular data classification system. Provided these two requirements are satisfied, the Sorting technique consists of four analysis steps:

1. Review the informational structure of the data
2. Search for patterns or clues
3. Sort to uncover trends and anomalies
4. Review and re-review as necessary

⁷⁰ A Tradecraft Primer: Basic Structured Analytic Techniques. Defense Intelligence Agency. March 2008, pp. 33-35.

⁷¹ Jones, Morgan D. *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving*. New York: Three Rivers, 1998. Print.

Tips

- Improper sorting can hide valuable insights as easily as illuminating them. Standardizing the data being sorted is imperative. Working with an analyst with experience in sorting can avoid this pitfall in most cases.
- Get others to review the sorted information to increase the brainstorming opportunities and for new ways of sorting the data to gain insight. Remember that correlation is not the same as causation.
- Return to sorting anytime during the analysis when new insights are gained and sorting can either support or negate the insight.

V.1. SORTING STEPS

Step 1: Review the informational structure of the data

Review how information is broken down (e.g., categories, factors) to determine which category or combination of categories might provide insight into the problem being studied. Place data into a spreadsheet or database, using as many fields (columns) as necessary to accommodate the factors in a factor-based model or the ontology of a data classification system. List each of the facts, pieces of information, or hypotheses involved in the problem that you may want to use in your sorting schema (can use paper, white board, movable Post-it papers, or other means).

Step 2: Search for patterns or clues

Review the listed facts/information/hypotheses in the database or spreadsheet to identify key fields that may allow you to uncover possible patterns or groupings. Those patterns or groupings then illustrate your schema categories and can be listed as header categories. For example, if you are examining terrorist activity and notice that most attacks occur in hotels and restaurants, but the times of the attacks vary, “Location” is the main category; while date and time are secondary categories.

Step 3: Sort to uncover trends and anomalies

Look for any insights, trends, or oddities. Good analysts notice trends; great analysts notice anomalies.

Step 4: Review and re-review as necessary

Review and re-review as necessary your sorted facts, information, or hypotheses to see if there are alternative ways to sort them. List any alternative sorting schema for your problem. One of the most useful applications of this technique is to sort according to multiple schemas and examine results for correlations between data and categories. For example, you notice that most terrorist attacks that happen in hotels also happen in June.

V.2. ILLUSTRATIVE EXAMPLES

The following examples were taken from the DIA Tradecraft Primer on Structured Analytic Techniques.⁷²

Example 1

Are a foreign adversary's military leaders pro-U.S., anti-U.S., or neutral on their attitudes towards U.S. policy in the Middle East? Sort the leaders by factors determined to give insight into the issue, such as birthplace, native language, religion, level of professional education, foreign military or civilian/university exchange training (where/when), field/command assignments by parent service, political influences in life, political decisions made, etc. Then review the information to see if any parallels exist between the categories.

Example 2

Data from cell phone communications among five conspirators is reviewed to determine the frequency of calls, the patterns in calls to discover the key communicator, any pattern in the change in frequency of calls prior to a planned activity, dates and times of calls, etc.

Example 3

Analysts are reviewing all information related to an adversary's WMD program. Electronic Intelligence (ELINT) reporting has over 300,000 emitter collections over the past year alone. The analysts sort the data by type emitter, dates of emission, and location shows varying increases and decreases of emitter activity with some minor trends identifiable. The analysts filter out all collections except those related to air defense. The unfiltered information is sorted by type of air defense system, location, and dates of activity. Of note, is a period where there is an unexpectedly large increase of activity in the air defense surveillance and early warning systems. The analysts review relevant external events and find that a major opposition movement outside the country held a news conference where it detailed the adversary's WMD activities, including locations of the activity within the country. The air defense emitters for all suspected locations of WMD activity, including several not included in the press conference, increased to a war level of surveillance within 4 hours of the press conference. The analysts reviewed all air defense activity locations that showed the increase assumed to be related to the press conference and the WMD programs and found two locations showing increased activity but not previously listed as WMD related.

These new locations were added to collection planning to determine what relationship if any they had to the WMD program.

⁷² A Tradecraft Primer: Basic Structured Analytic Techniques. Defense Intelligence Agency. March 2008, pp. 33-35.

This page is intentionally blank.

APPENDIX W. SYSTEM DESCRIPTION METHODOLOGY

What is it?	This System Description Methodology provides an approach for completely describing a system of interest. Typically used before performing a risk analysis, the outcome from this methodology is a model of a system of interest defined in terms of its input, output, and state variables. Much of this methodology is derived from Chapter 2 of a textbook on risk analysis by Yacov Haimes ⁷³ and Chapter 1 of a textbook on systems analysis by George Klir. ⁷⁴
Why use it?	Helps define the scope. Applying this methodology prior to performing a risk analysis will help in defining the scope of what is and is not considered in the analysis, what outcomes are of concern, and how failure (whether accidental or deliberate) of system components maps to these outcomes.
Timing	Develop and Define Phases: This methodology should be used when a complete understanding of a system in terms of its inputs, outputs, and inner workings is required. For instance, this methodology must be performed prior to any type of systems analysis, including Fault Tree Analysis (Appendix J) and Failure Modes and Effects Analysis (Appendix I).
Steps	The overall approach for this methodology is comprised of the following seven steps: <ol style="list-style-type: none">1. Define the objective(s) of the system2. Articulate the success scenario(s)3. Define system failure4. Define all relevant output variables5. Define all relevant input variables6. Define all relevant state variables7. Identify the components of the system and relate them to the input, output, and state variables
Tips	Resolution of the description. The resolution of the description should align or match the resolution necessary to properly inform decision making. Lower resolution system models do not provide adequate detail to inform decisions and higher resolution models add unnecessary complexity and waste analytical resources. Care should be taken to balance available resources and information requirements with model resolution.

⁷³ Haimes, Yacov Y. *Risk Modeling, Assessment, and Management*. Hoboken: John Wiley & Sons, 2009. Print.

⁷⁴ Klir, George J. *Facets of Systems Science*. New York: Kluwer, 2001. Print.

W.1. SYSTEM DESCRIPTION METHODOLOGY STEPS

Step 1: Define the objective(s) of the system

The objectives of the system are typically couched in terms of a crisply defined level of performance, such as “generate greater than 10MW of electricity persistently” for a power plant or “maintain a 90% response time to 3 minutes and below for major emergencies” in the case of an emergency response unit.

- All stated objectives should be based on verifiable metrics. That is, an objective such as “keep people happy” should only be specified if there is some way to measure happiness.
- Moreover, all objectives should be stated in crisp language. For example, “protect the fort” is too vague of an objective because it is unclear what the word “protect” means. An alternative way of saying this is “deny success to adversaries that attempt to attack the fort.”
- For any given system there may be more than one objective.

Step 2: Articulate the success scenario(s)

Building on the objective(s) defined in Step 1, this step seeks to articulate a complete set of success scenario(s). A success scenario is a concise statement of how a system must perform based on three dimensions, Capability, Duration, and Environment (CDE):

- Capability – specifically, what is the system supposed to do?
- Duration – for how long?
- Environment – under what conditions?

Successful performance demonstrating better-than-required capability, success in harsher environments, and for extended periods of time fall within the scope of the success scenario. That is, the success scenario defines the boundary between failure and success.

Step 3: Define system failure

Failure of a system is defined as an undesirable deviation in performance that causes the system to function at a level less than called for in the success scenario. Failure can be in terms of inadequate capability, inability to function at the required level in a particular environment, or for a less than desired amount of time.

It may be helpful here to define different gradations of failure, such as “partial” or “complete” failure, or perhaps “minor” or “major” or “catastrophic” failure. For each gradation, a statement of what failure at this level means should be made.

Note that for security systems, it is more common to discuss security system failure in terms of security system defeat.

Step 4: Define all relevant output variables

An output variable is one that enables an assessment as to how the system is performing. For example, if the objective is “response time less than 3 minutes,” the appropriate output variable to measure is “response time.” Depending on the nature of the success scenario, there may be multiple output variables.

Step 5: Define all relevant input variables

An input variable is one that feeds into the system to contribute to its performance. Input variables come in a variety of types, including:

- Decision variables: inputs that are controllable by the decision maker
- Environmental variables: inputs from the environment, some of which might be random
- Exogenous variables: inputs from outside the system

Depending on the nature of the system and its objectives, there may be multiple input variables.

Step 6: Define all relevant state variables

A state variable is an intermediate variable that describes the properties of the system at any given time. State variables are influenced by inputs and internal processes. State variables then directly influence the values of the outputs and thus whether the system performs in accordance with the success scenario. For example, a state variable in the emergency response situation might be number of available responders at a given time and number of active incidents. Combined, these two variables influence the ability of the system to respond to an incident.

Step 7: Identify the components of the system

In this step, all components of a system are identified, to include persons, objects, organizations, and all other objects. This is followed up with a complete discussion of how each “thing” identified relates to the other things in the system, and in particular what inputs each thing receives and how its individual performance influences the state variables.

This page is intentionally blank.

APPENDIX X. WEIGHTED RANKING

What is it? Weighted Ranking is a technique for ranking and prioritizing different events, vulnerabilities, hazards, threats, countermeasures, or other objects with respect to two or more value criteria. This technique can be used to rank and order threats, hazards, vulnerabilities, and countermeasures. A technique used by an individual or group to gain confidence in the assessment of available alternatives by weighting criteria in importance from the decision maker's point of view.^{75, 76}

Why use it? Weighted Ranking adds validity to an assessment of alternatives, options, and hypothesizes by mitigating bias and mindset in comparison to an analyst's intuition that results in the unsystematic and therefore inconsistent use of criteria. The results of the systematic approach provide transparency of the derivation and logic of the assessment to customers who may otherwise question the assessment or key judgments.

Timing Assess and Enhance Phases: Weighted Ranking should be used anytime the topic is important enough to warrant the investment of time and there is a need for transparency in the reasoning used to derive the assessment. In intelligence analysis, each criterion used in the technique must be selected and given a weighted importance from the adversary decision maker's point of view. The insight gained on how each criterion will affect the final outcome allows for a clear, persuasive presentation and argumentation of the assessment.

Steps The Weighted Ranking methodology is comprised of the following eight steps:

Step 1: Begin to fill the matrix

Step 2: Develop independent criteria

Step 3: Pair rank the criteria

Step 4: Count the votes

Step 5: Complete options matrix

Step 6: Pair rank options

Step 7: Count the votes

Step 8: Sum all final markets

⁷⁵ *A Tradecraft Primer: Basic Structured Analytic Techniques*. Defense Intelligence Agency. March 2008, pp. 63-67.

⁷⁶ Jones, Morgan D. *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving*. New York: Three Rivers, 1998. Print.

Tips

- Weighted Ranking takes more time than many other basic analytic techniques and relies on a fair number of mathematical computations, which causes many analysts to avoid the technique.
- Use a different color for each criteria and alternative during the pair ranking to make the choices transparent (easy to review or recreate).
- Weighted Ranking helps mitigate bias and mindset when the analyst using it faithfully follows the method and treats each step as equally important to the outcome. The technique can be used by a group working together as long as a group facilitator keeps the process on track. The validity of the weighting of the criteria can be enhanced by the group through discussions sharing insight into the adversary decision maker's purpose and point of view.

X.1. WEIGHTED RANKING STEPS

There are eight steps to accomplish a Weighted Ranking review of alternative options being assessed.

Step 1: Begin to fill the matrix

Take the alternatives, options, or hypothesis generated or another process to fill in the first column of a matrix under the column heading of Options.

Step 2: Develop independent criteria

On a separate sheet of paper or file, develop a comprehensive list of independent criteria the adversary would be likely to use to determine which option to select. List the criteria in a column with one criterion per line. Notice that the context of the time, place, and objectives of the action being reviewed should be considered in the development of the criteria.

Step 3: Pair rank the criteria

Pair ranking requires each item being ranked to be compared with every other item and the selection of one over the other. Start with the first criterion in the list and compare it to the second criterion. Place a mark (1 or X) next to the criterion selected as the more important between the two. Next compare the first criterion with the third. Again mark the more important of the two. Once the first criterion has been ranked against all of the others, go to the second criterion and compare it with the third, placing a mark next the one judged most important. Then rank the second criterion with the fourth, and so on until it has been ranked against the remaining criteria in the list. Note that the second and succeeding criteria are not ranked against criteria on the list listed above them because that was accomplished when those criteria were going through the process. Continue to rank each criterion with those below it in the list until the list is completed.

Step 4: Count the votes

Count the marks or votes for each criterion in the list, and write the total to the right of the criterion and marks. Review the totals of each criterion and determine how many of the listed criteria to use in the Weighted Ranking matrix. Note that more than five or six criteria rarely provide sufficient difference to be worth the time and expertise. Count the total number of votes or marks received by the criteria selected to use to determine which option is the most likely. Divide the number of votes received by each selected criterion by the total number of votes for all selected criteria. For example, if the total number of votes for the selected criteria is 15 and the first criterion received 5 votes, divide 5 by 15 to get 33 percent, and the second criterion received 4 votes then divide 4 by 15 to get 27 percent (rounded up 26.7 percent to the next full number) and so on through the selected criteria. Make sure the total of the percent for the criteria adds up to exactly 100 percent by rounding off the figures as required.

Step 5: Complete options matrix

Enter the criteria in the options matrix as column headings starting with the second column. Note that the first column heading is Options. Include the percentage for each criterion with it in the column heading. The order that the criteria are entered is not important, but confusion can be avoided if the criterion with the largest percentage is entered in the first column and the remainder added in descending order.

Step 6: Pair rank options

Pair rank the options based on the first criteria from the point of view of the adversary decision maker. The pair ranking is accomplished exactly like the procedure used in Step Four to rank the criteria. Compare the first option with the second option and determine which option most meets the criteria. Then place a mark (I or X) in the box at the intersection for best option for the criteria. After pair ranking all of the options for the first criterion, move to the second criterion (column) and pair rank all of the options against that criterion and so on until all criteria are used to pair rank the options.

Step 7: Count the votes

Count the number of marks (votes) in each square in the matrix under the criteria and write the number in the square. Then multiple the number by the weight of the criteria (the percentage listed with the criterion at the top of the column). Write the product (result of the multiplication) in the square as well.

Step 8: Sum all final markets

Once all squares with marks have been multiplied by the percentage for that criterion and placed in the appropriate square, add the product (result of the multiplication) in each square for each option (row). That is, add all of the final numbers in each square across the row and place the total in the final column for that option (row). This number can be larger than 1 (e.g., 2.58). The row with the largest total is the most likely option.

End by making a sanity check of the results and review the impact of the weighted criteria on the final result. This review should provide the insight needed to present the results in a clear and persuasive manner to customers. At a minimum, it will provide insight to the analyst on the interaction of the criteria from the point of view of the adversary decision maker.

X.2. ILLUSTRATIVE EXAMPLE

The following example was taken from the *DIA Primer on Structured Analytic Techniques*.⁷⁷

A major adversary is suspected of constructing a new chemical agent manufacturing facility to replace the aging and inefficient facilities currently in use. Reports of various sites being considered have surfaced from numerous sources. To select the most likely location, the Weighted Ranking technique is used to provide insight into the issue.

Step 1

The reported sites and two suspected potential locations are placed in the matrix.

OPTIONS					Total
Lumbadca					
Buscanna					
Separata					
Raticana					
Lemitica					

Step 2

Develop a list of possible choice criteria. For example:

- Security
- Transportation
- Work Force
- Electric Power
- Water
- Fuel
- VIP Housing
- Waste Disposal
- Recreation Area

⁷⁷ A Tradecraft Primer: Basic Structured Analytic Techniques. Defense Intelligence Agency. March 2008, pp. 21-24.

Step 3

Pair rank the criteria.

Security	IIII	5*
Transportation	III	3
Work Force	III	3
Electric Power	IIII	6*
Water	IIIIII	7*
Fuel	II	2
VIP Housing	I	1
Waste Disposal	IIII	6*
Recreation Area		0

Step 4

Total the votes for each criterion and mark those with asterisk selected for use in the options matrix.
Calculate the percentage weight for each criterion.

Security	5
Electric Power	6
Water	7
Water Disposal	6
Total	24

$$7 \text{ div by } 24 = .29$$

$$6 \text{ div by } 24 = .25$$

$$5 \text{ div by } 24 = .21$$

Step 5

Enter the criteria in the matrix column headings.

OPTIONS	Water .29	Elec Power .25	Waste .25	Security .21	Total
Lumbadca					
Buscanna					
Separata					
Raticana					
Lemitica					

Step 6

Pair rank each option by each criterion.

OPTIONS	Water .29	Elec Power .25	Waste .25	Security .21	Total
Lumbadca	I	III	II	II	
Buscanna	III	II	I	I	
Separata	II	I	III	III	
Raticana		III	III		
Lemitica	III			III	

Step 7

Count the number of votes for each option under the criteria and write the number in the square. Then multiple the number of votes by the weight of the criteria (the percentage listed with the criterion at the top of the column). Write the product (result of the multiplication) in the square.

OPTIONS	Water .29			Elec Power .25			Waste .25			Security .21			Total
Lumbadca	I	1	.29	III	3	.75	II	2	.5	II	2	.42	
Buscanna	III	3	.87	II	2	.50	I	1	.25	I	1	.21	
Separata	II	2	.58	I	1	.25	III	4	1.00	III	3	.63	
Raticana		0	0	III	4	1.00	III	3	.75		0	0	
Lemitica	III	4	1.16		0	0		0	0	III	4	.84	

Step 8

Add the product (result of the multiplication) in each square for each option (row) and place the total in the final column for that option (row). This number can be larger than one. The row with the largest total is the most likely option.

OPTIONS	Water .29			Elec Power .25			Waste .25			Security .21			Total
Lumbadca	I	1	.29	III	3	.75	II	2	.5	II	2	.42	1.96
Buscanna	III	3	.87	II	2	.50	I	1	.25	I	1	.21	1.83
Separata	II	2	.58	I	1	.25	III	4	1.00	III	3	.63	2.46
Raticana		0	0	III	4	1.00	III	3	.75		0	0	1.75
Lemitica	III	4	1.16		0	0		0	0	III	4	.84	2.00

Note that Separata is not highly regarded against the most important criteria (Water), but when the remainder of the criteria is considered, it is by far the best location for the new facility. Although this technique will not ensure that the analyst has selected the site of the future plant, he or she will have a great deal of insight into the issue that probably would not be considered systematically without the use of the technique.

X.3. PAIRWISE RANKING

What is it? Pairwise Ranking is a structured analytic technique for ranking a small list of items in priority order, whether by importance, preference, or other measure of value.⁷⁸

Why use it? When performed as a group, pairwise ranking helps the group come to consensus.

Timing Assess and Enhance Phases: Use pairwise ranking when you need to quickly rank order a small list of items.

Steps The Pairwise Ranking technique consists of the following five steps:

1. Identify a list of items to rank
2. Construct a pairwise matrix
3. Rank each pair
4. Count the number of times each item is preferred
5. Rank items based on count

Tips

- Pairwise ranking is a very useful tool, as long as the criteria are really asked for and noted down.
- The tool can be used in groups as well as in interviews with individuals.
- The number of items to be ranked should not exceed 5-6. Otherwise the procedure becomes too lengthy and the concentration of the group will decrease.
- Pairwise ranking does not give all information, which might be needed (e.g. different importance of criteria).⁷⁹

X.3.1. Pairwise Ranking Steps

Step 1: Identify a list of items to rank

This can be done using one or more brainstorming techniques.

⁷⁸ *Pairwise Ranking*. Concordia University. <<http://web2.concordia.ca/Quality/tools/18pairwise.pdf>>.

⁷⁹ “Pairwise/ Preference Ranking.” FAO. <http://www.fao.org/Participation/ft_more.jsp?ID=3022>.

Step 2: Construct a pairwise matrix

Each box in the matrix represents the pairing of two items. An example pairwise matrix for five items is shown below.

	1			
2		2		
			3	
3				4
4				
5				

Step 3: Rank each pair

Part One (3-1): For each pair, have the group, either alone individually or in a group consensus-oriented discussion, determine which of the two items is preferred.

Part Two (3-2): For each pair, write the number of the preferable item in the appropriate box. Repeat these two steps until all boxes are filled.

1 and 2 compared:

2 is better.

1 and 3 compared:

1 is better.

4 and 5 compared:

5 is better.

	1			
2		2		
			3	
3				4
4				
5				

	1			
2		2	2	
				3
3				
4				4
5				

...and so on
until...

	1			
2		2	2	
				3
3			1	
4			2	
5			5	

Step 4: Count the number of times each item is preferred

Write down the tally for each item in a table.

Alternative	1	2	3	4	
	2	3	1	0	
Count					
Rank					

Alternative 5 appears 4 times in the matrix.

Step 5: Rank items based on count

Rank the alternatives by the total number of times they appear in the matrix. To break a tie (where two ideas appear the same number of times), look at the box in which those two items are compared. The idea appearing in that box achieves the higher ranking.

	Alternative e	1	2	3	4	
Alternative e ranks 1st overall.	Count	2	3	1	0	
	Rank	3rd	2nd	4th	5th	

X.3.2. Illustrative Example

A QAT was asked to recommend sites for testing a pilot program of their recommendations. A feasibility study produced a list of six possible locations. The team then used pairwise ranking to determine that ATTC Elizabeth City, NC was best suited for this particular test.

1. TRACEN Petaluma
2. RTC Yorktown
3. TRACEN Cape May
4. ATTC E-City
5. ATC Mobile
6. Academy

		1				
2	2	2				
3	1	3	3			
4				4		
5	5	5	5		5	
6	1	6	6		5	

Alternative	1	2	3		5	6
Count	2	1	1		4	2
Rank	3rd	6th	5th		2nd	4th

This page is intentionally blank.

APPENDIX Y. WORK BREAKDOWN STRUCTURE

What is it? A Work Breakdown Structure (WBS) is a dynamic process for defining the products of a project and their relationships. Generally, WBS uses a tree diagram/structure diagram to show the resolution of overall requirements into increasing levels of detail. WBS allows a team to accomplish its general requirements by partitioning a large task into smaller components and focusing on work that can be more easily accomplished.⁸⁰

Why use it?

- Provides a necessary framework:** A WBS provides project planners with a tool to for developing detailed cost estimations as well as a mechanism for cost control.
- Produces a schedule:** One of the primary benefits of a WBS is the production of a project timeline and schedule tasks and events.
- Early detection:** While using a WBS, project management is able to track a work stream's progress. This provides them with a way to identify problems in the process such as scheduling conflicts, over-allocation of resources, and scope creep.

Timing WBS should be used in all projects for planning and management purposes. It is used to help project managers map out the project life cycle in its entirety. This methodology can be used in any size project to help organize the sections and subsections in a logical, chronological manner.

Steps The WBS process is comprised of the following two steps:

Step 1: Identify the Objective
Start by listing the final goal or end product at the top of a page or whiteboard.

Step 2: Divide the Objective Into Greater Detail

- Part One (2-1):** With your group, identify primary categories that directly lead into your end product. List them below the end product.
- Part Two (2-2):** Break down each level into more specific tasks.
- Part Three (2-3):** Review the WBS and consider any cause and effect relationships between consecutive levels. Make sure nothing important is left out.

⁸⁰ *Work Breakdown Structure*. Concordia University. <<http://web2.concordia.ca/Quality/tools/30workbreakdownstructure.pdf>>.

Tips

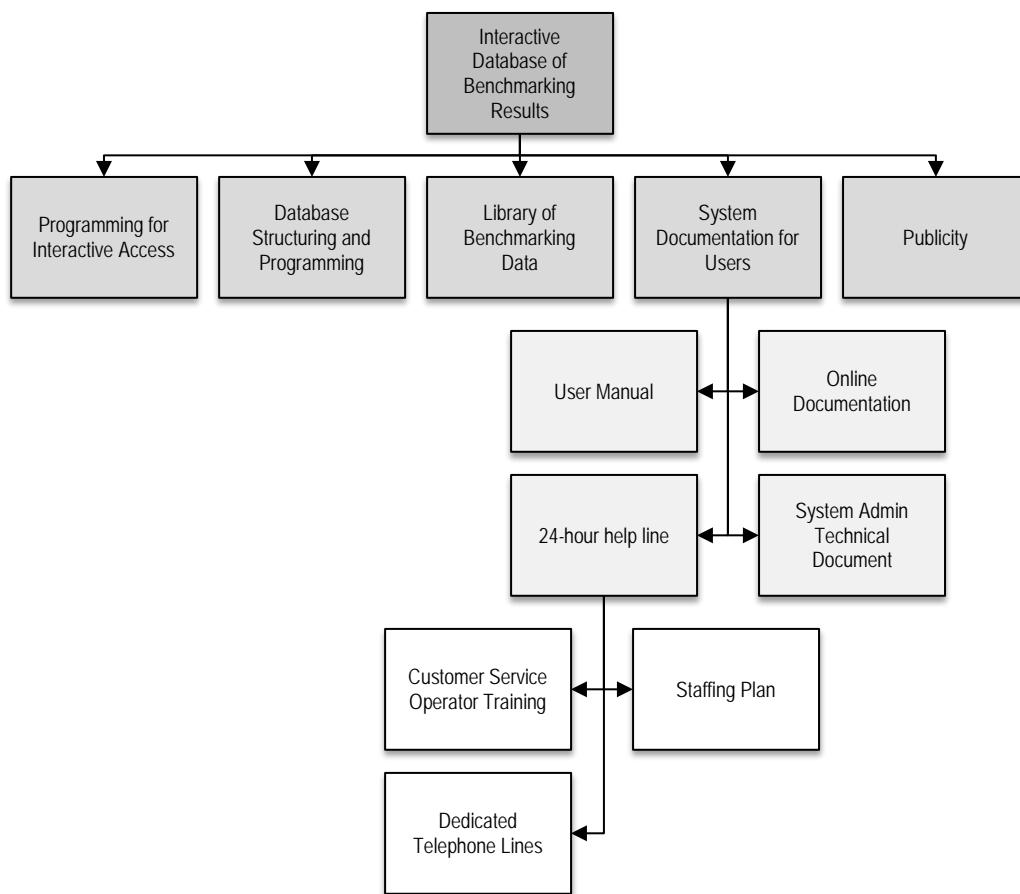
Planner must have extensive knowledge: The individual or team developing this methodology must have an extensive knowledge of the project and its objectives. If there is not a shared understanding of the primary goals of the project the WBS will not accurately reflect these plans.

WBS should be outcome-oriented: Many project plans require formal changes to the plan. For this reason the WBS should be written to express the desired outcome not the method for which the outcome will be created. If project planners decide to blend the objective with the means for achieving that objective it may become difficult to control changes. In short, the WBS does not identify the method or means for achieving a goal, just the goal.

Y.1. ILLUSTRATIVE EXAMPLE

Example 1

Below is an example of a Work Breakdown Structure:



Example 2

Below is a variation of a Work Breakdown Structure known as an Action Plan or Gantt Chart.

ID	Task Name	Duration	23-Apr-00					30-Apr-00					7-May-00					14-May-00					21-May-00					28-May-00				
			S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S		
1	Get final report from PS	5 days	Wilbur																													
2	Get blueprints for old hs	1 day	Wilbur																													
3	Time-motion study of e	2 days								Orville, Production supervisor																						
4	Design electrical and pn	4 days					Wilbur																									
5	Schedule down-time w	2 days					Orville			Orville, Production supervisor																						
6	Schedule truck to picku	1 day					Orville																									
7	Inform PSU about picku	2 days					Orville																									
8	Schedule contractor for	1 day								Wilbur																						
9	Transport hardware ho	2 days								Trucking Company																						
10	Shut down production l	1 day								Production supervisor																						
11	Remove old hardware 2	days									Shop machinist																					
12	Store old hardware (us	10 days									Wilbur																					
13	Renovate electrical and	2 days									Contractor for electrical and pneumatic																					
14	Install new hardware 3	days									Shop machinist																					
15	Shake-down test by en	2 days										Wilbur																				
16	Training for production	2 days										Wilbur, Orville																				
17	Shake-down test by ph	2 days										Orville, Production supervisor																				
18	Training for production	1 day										Wilbur, Orville																				
19	Restart production 1 day											Orville																				
20	Time-motion study of n	2 days										Production supervisor																				
21	Scrap old hardware 3	days										Orville																				

This page is intentionally blank.

THREAT AND HAZARD NETWORKS

APPENDIX Z. THREAT AND HAZARD NETWORKS

Networks are available as references that visually depict pre-attack activities, cascading effects of a threat or hazard, or a combination thereof.

APPENDIX Z

NETWORKS OVERVIEW	Z-3
GENERAL THREAT NETWORK.....	Z-5
Z.1. General Threat Network (Pre-Attack)	Z-6
HAZARD NETWORKS.....	Z-7
Z.2. Airplane Crash.....	Z-8
Z.3. Biological Attack.....	Z-9
Z.4. Broken Water Line(s).....	Z-10
Z.5. Communications Disruption	Z-11
Z.6. Cyber Attack	Z-12
Z.7. Dam/Levee Failure	Z-14
Z.8. Drought	Z-15
Z.9. Earthquake.....	Z-16
Z.10. Environmental Loss.....	Z-17
Z.11. Erosion	Z-18
Z.12. Evacuation.....	Z-19
Z.13. Extreme Heat.....	Z-20
Z.14. Fire	Z-21
Z.15. Flooding	Z-22
Z.16. Hurricane.....	Z-23
Z.17. Improvised Explosive Device	Z-24
Z.18. Injury	Z-25
Z.19. Landslide	Z-26
Z.20. Nuclear Incident / Radiological Emergency	Z-27
Z.21. Pandemic / Epidemic.....	Z-28
Z.22. Power Disruption (Electric).....	Z-29
Z.23. Property / Structural Damage	Z-30
Z.24. Passenger Rail Collision / Derailment.....	Z-31
Z.25. Shooting Incident	Z-32
Z.26. Snow.....	Z-33
Z.27. Spread of Hazardous Materials	Z-34
Z.28. Supply Chain Disruption.....	Z-35
Z.29. Thunderstorm	Z-36
Z.30. Transportation Systems Disruption	Z-37
Z.31. Tree Damage	Z-38
Z.32. Vehicle Accident.....	Z-39
Z.33. Water Contamination	Z-40
Z.34. Water Systems Disruption.....	Z-41
Z.35. Wind.....	Z-42
Z.36. Winter Storm	Z-43
SPECIAL EVENT NETWORK	Z-44
Z.37. Special Event / Mass Gathering	Z-45
GLOSSARY OF CYBER TERMINOLOGY.....	Z-46
Z.38. Glossary of Cyber Terminology	Z-47

NETWORKS OVERVIEW

This Appendix features graphics – referred to as “networks” – that illustrate the relationships between pre-attack activities associated with a terrorist or criminal threat and between downstream hazards associated with a certain event or hazard, thus showing cause and effect (or cause and consequence). Simply put, networks visually depict those activities and cascading effects related to the occurrence of an event or hazard. Like all content of the Continuity Risk Toolkit, this information is intended to serve as helpful reference material for conducting risk analyses and enhancing risk-informed decision making. Networks may aid in framing questions for subject-matter experts and stakeholders, developing and validating continuity and response plans, and crafting exercise scenarios.

The networks are kept at a general level, thus stakeholders should apply knowledge of their organizations and of the jurisdictions in which those organizations are located to a given network in order to determine the extent to which certain consequences or cascading effects may impact them. Notably, the networks included in the Continuity Risk Toolkit are not exhaustive illustrations of all consequences of a given event, nor do they represent all of the wide-ranging threats and hazards that may impact an organization. Various structured analytic techniques described in the Continuity Risk Toolkit, particularly brainstorming techniques, can aid in exploring the networks and their applicability to a given organization, jurisdiction, or system, as well as building on the baseline information provided in the networks. Organizations may opt to tailor these networks or to create additional network sketches representative of other hazards based on research and subject-matter expert elicitation to further inform risk analysis and risk management decisions.

The **general threat network** is depicted as a single network that applies to both terrorism and criminal acts. The threat network illustrates an adversarial operations process, also referred to as an attack process, and features numerous pre-attack activities. It represents the general flow of an attack process, starting with a person or group with intent to attack a target or trigger an incident.

The **general hazard network** depicts cause and consequence and is represented through network “slices” that visualize the linkages (causal relationships) between initiating events or causal hazards (cause) and downstream or outcome hazards (consequence). These “slices,” generally referred to as hazard networks, show a portion of the broader network as related to a given event or hazard. In many cases, the networks will link to one another to illustrate additional cascading effects.

The **Special Event Network** is a unique network in that it captures potential consequences of a special event or mass gathering and lists key factors to consider when planning for the effects of a special event.

As an added reference, color-coding of linkages is utilized in select hazard networks to indicate causal relationships that may directly impact Public Health and Safety (including loss of life) and Mission Disruption. Also, included in the upper right corner of select networks is a list of key commonalities and considerations that stakeholders should keep in mind when looking at the network as a whole, including events and hazards and select mitigation actions or countermeasures. These lists are not exhaustive, but highlight issues of importance as related to the effects of a given threat, event, or hazard.

The network graphics included in the Continuity Risk Toolkit are from FEMA’s The Full-Spectrum Risk Knowledgebase program, 2009-2014.

Below is a legend of the icons used throughout the networks.

Legend			
	Initiating Event		Downstream Hazard (consequence/impact)
	Downstream Hazard		Mitigation / Countermeasure
	Linkage (indicates causal relationship between hazards)		Non-Traditional Linkage (indicates a synonymous or "type thereof" relationship; may be blue, green, or red in color)
	Linkage that highlights Public Health and Safety issues		Linkage that highlights Mission Disruption issues
	Downstream Hazard which is an Initiating Event for another network		

GENERAL THREAT NETWORK

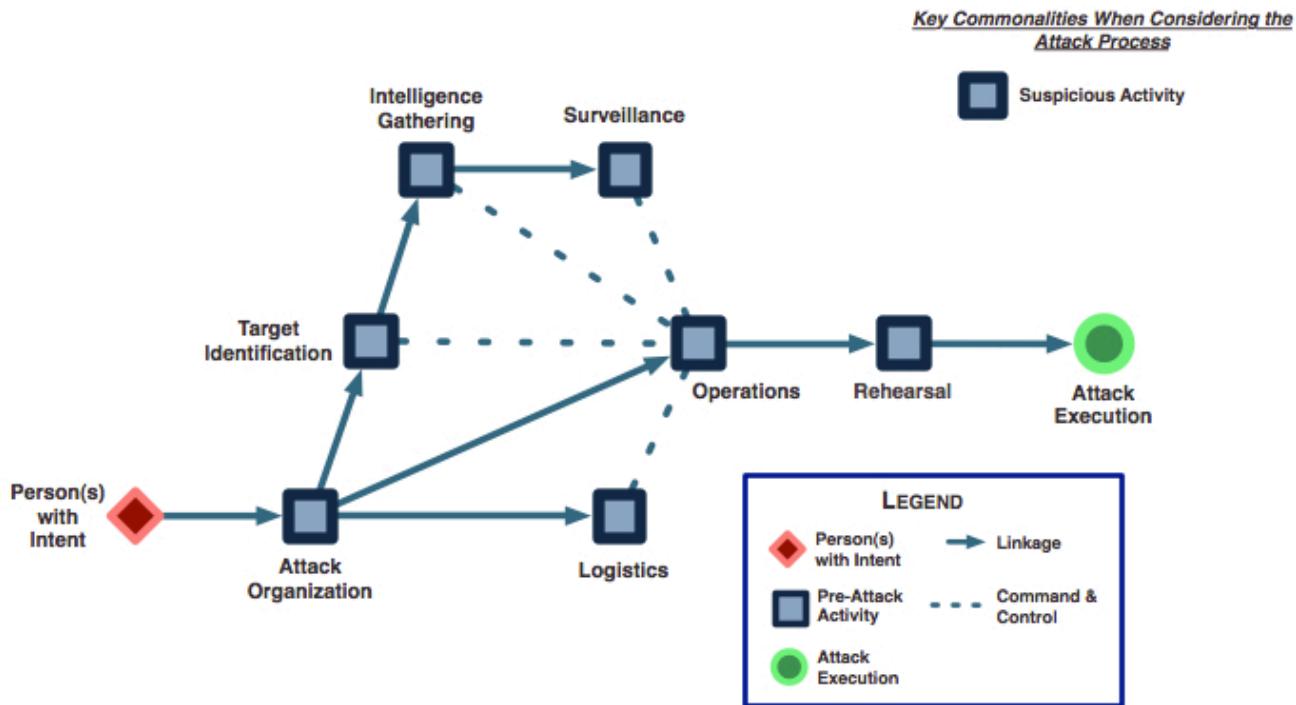
Z.1. GENERAL THREAT NETWORK (PRE-ATTACK)

Pre-attack activities are depicted below in the general threat network. This network illustrates an adversarial operations process, also referred to as an attack process. It applies to attacks of both a terrorist and criminal nature.

Each attack begins with a person or group with intent – the intent to attack a target or cause (trigger) an incident; if acting alone, without assistance, a person with the intent to attack is often termed a “lone wolf.” This is followed by the organization of the attack, to include formation of an attack team or group. The attack process culminates in attack execution, represented through numerous initiating events related to terrorism and crime. In general, an attack operation includes three stages, often outlined in an operational plan:

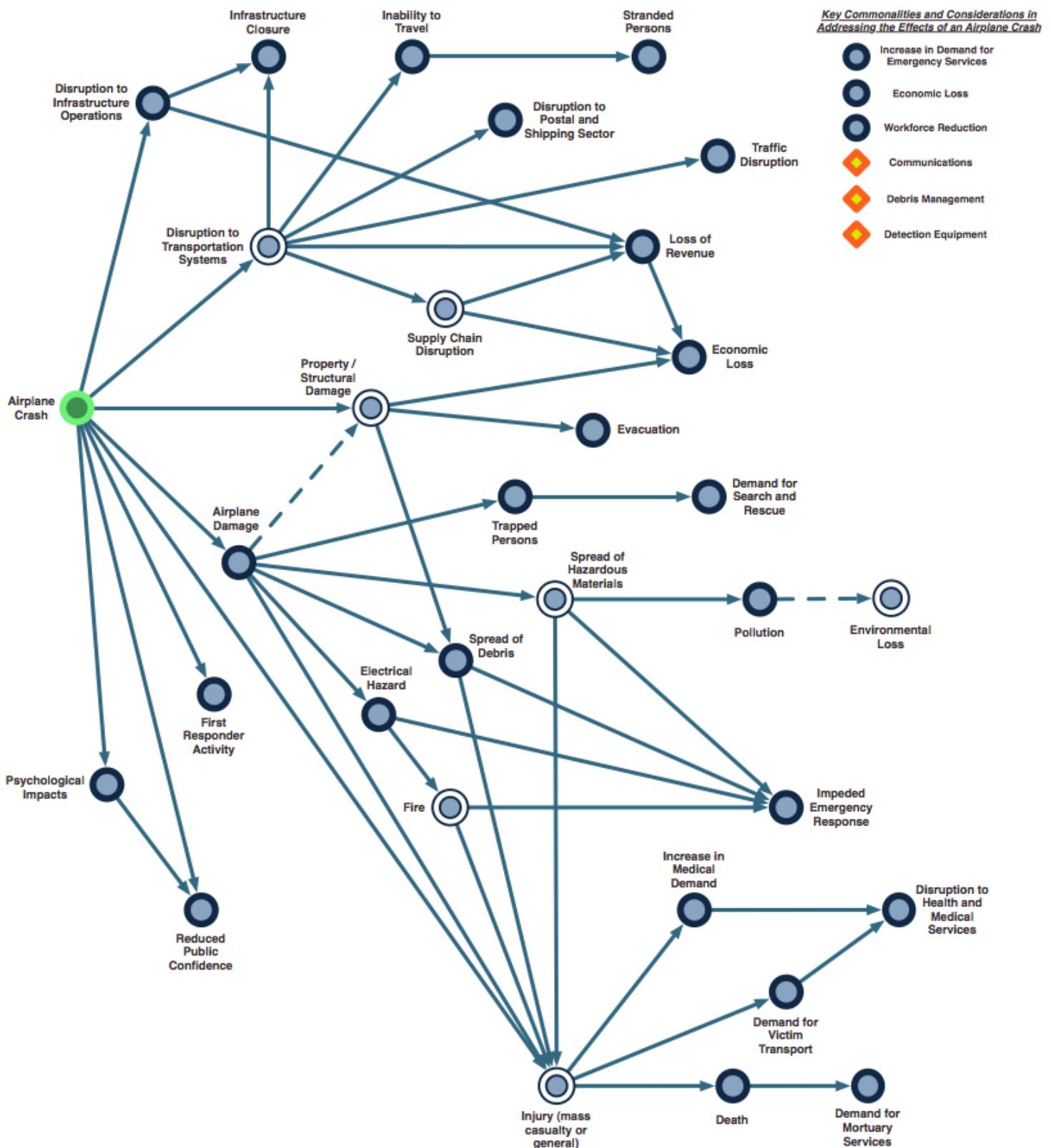
- Research (reconnaissance), which may consist of the Target Identification, Intelligence Gathering, and Surveillance activities
- Planning, which centers on the Operations and Logistics activities
- Execution, which consists of the Rehearsal activity and Attack Execution

Of note, many activities associated with the general threat network can be performed simultaneously. Suspicious activity may also be observed throughout the attack process and can be related to any of these other activities. The below network is intended to depict the basic flow of activities leading up to an attack or adversarial event and is not meant to show a true cascading effect.

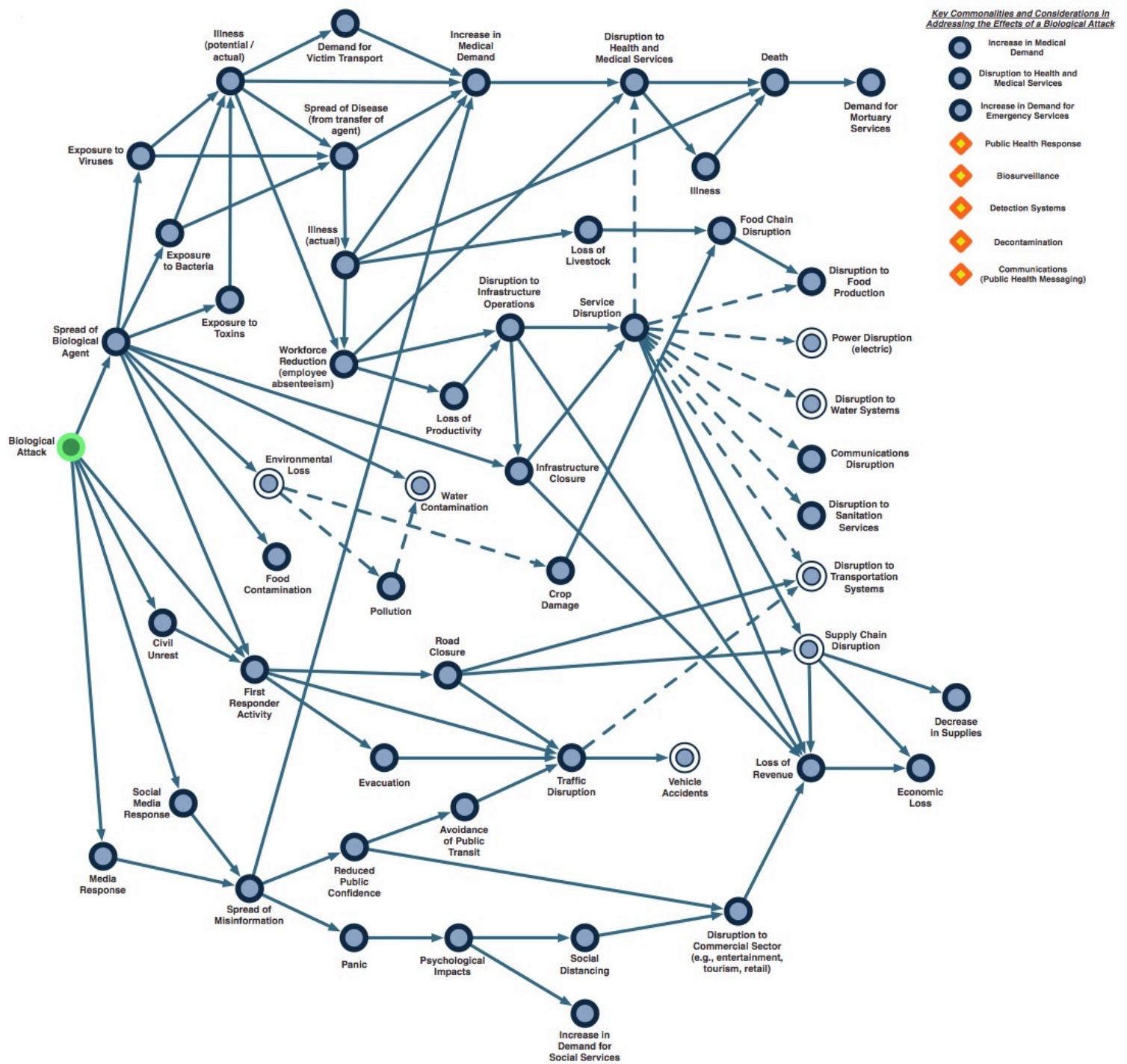


HAZARD NETWORKS

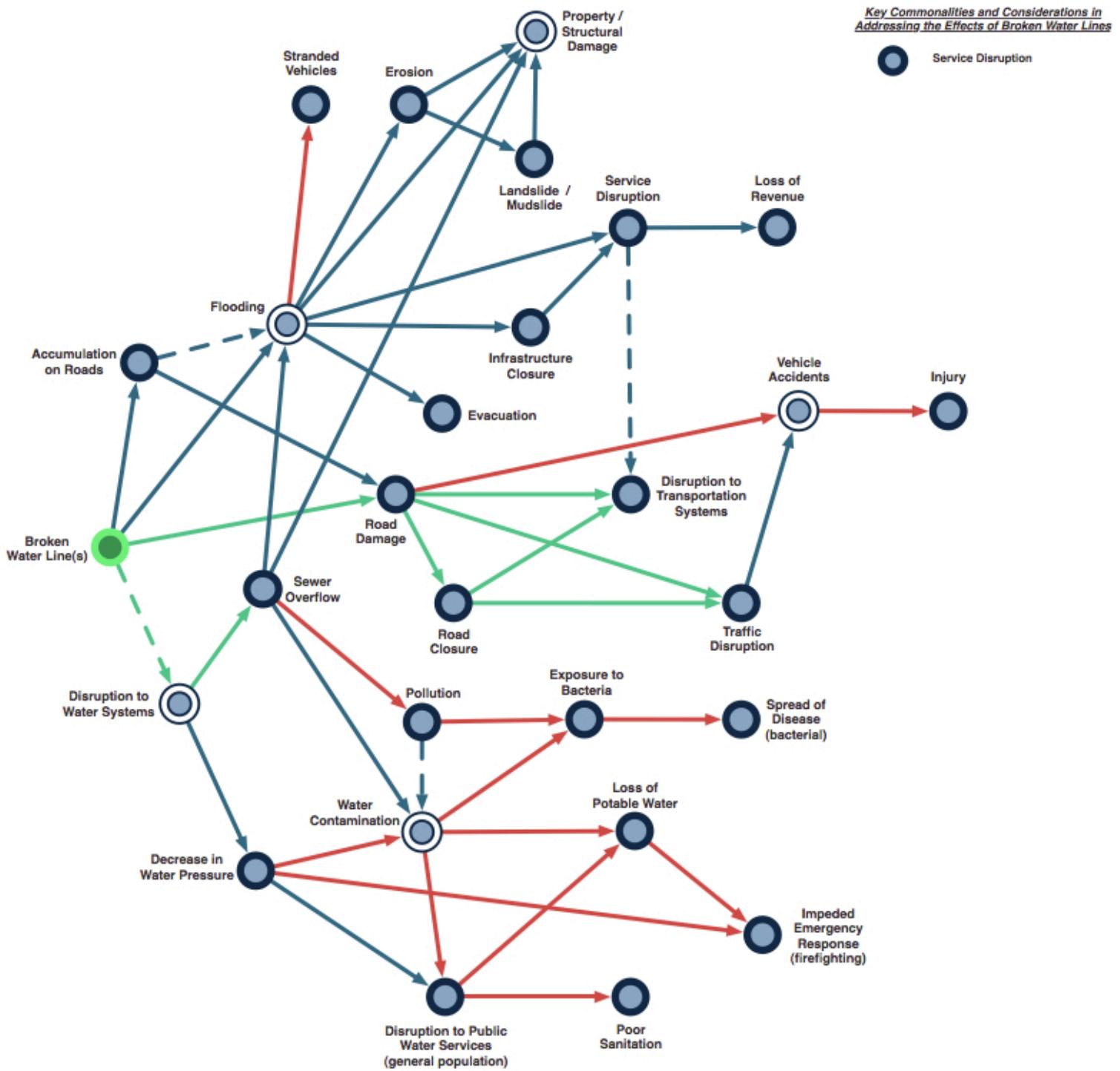
Z.2. AIRPLANE CRASH



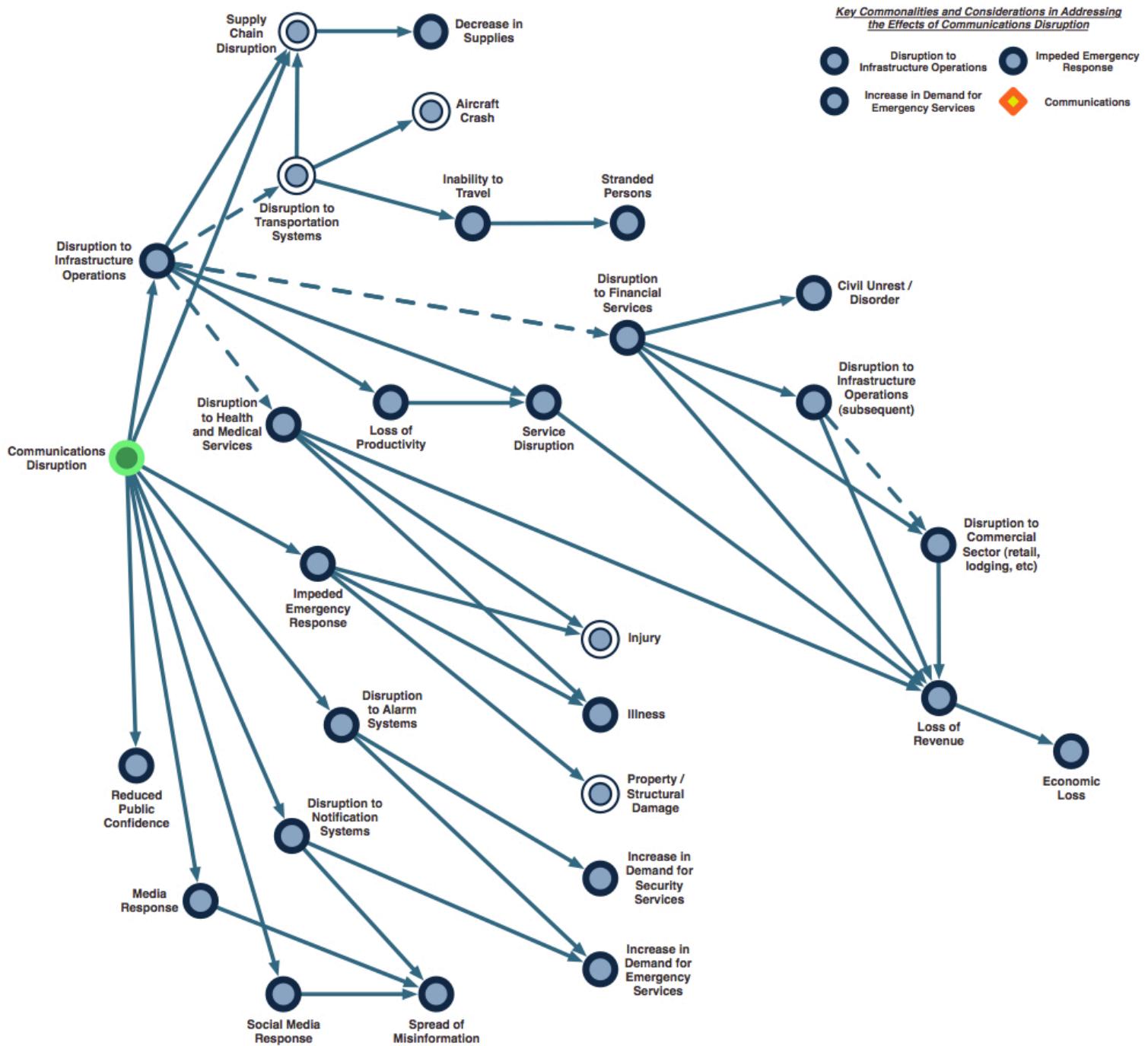
Z.3. BIOLOGICAL ATTACK



Z.4. BROKEN WATER LINE(S)

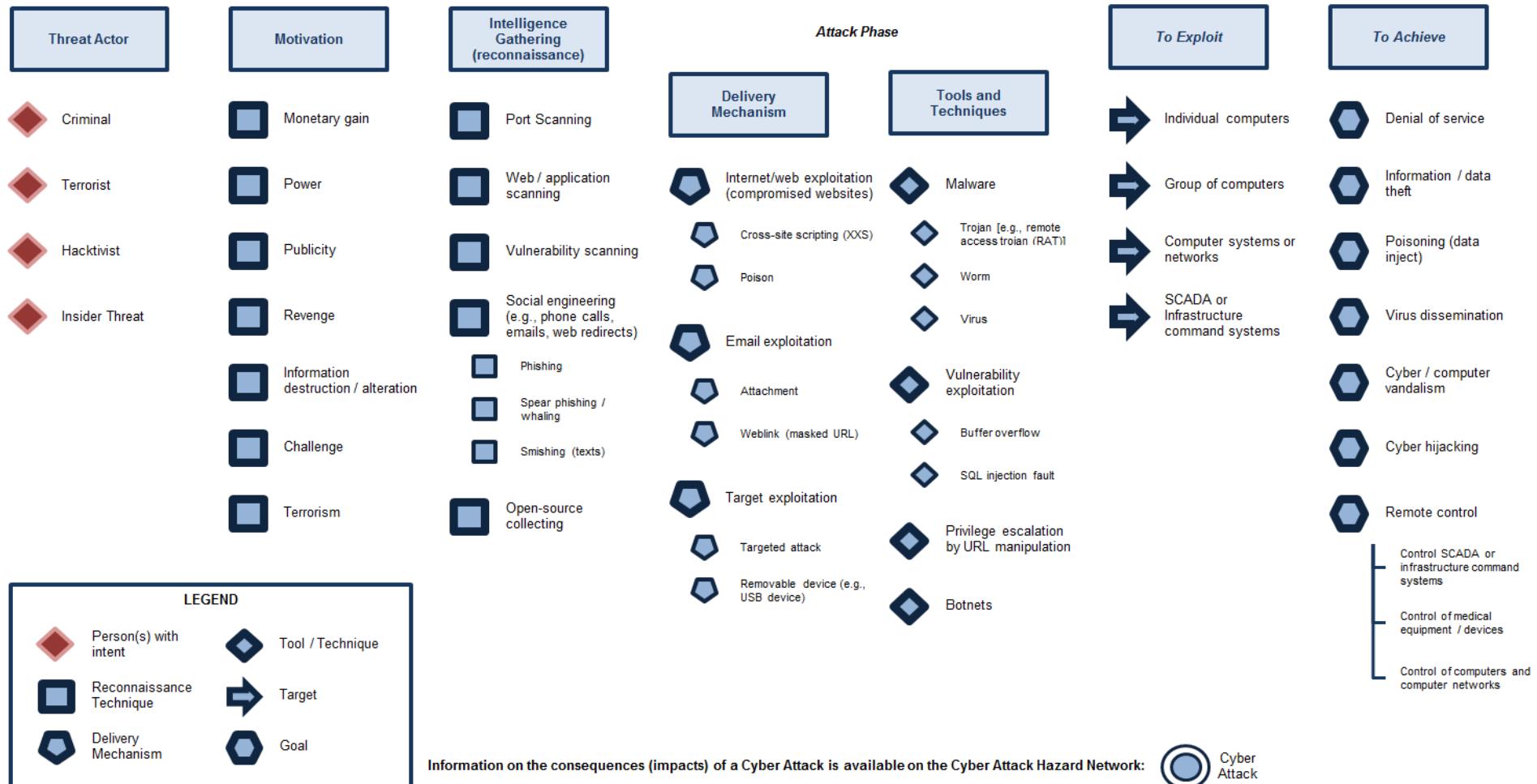


Z.5. COMMUNICATIONS DISRUPTION

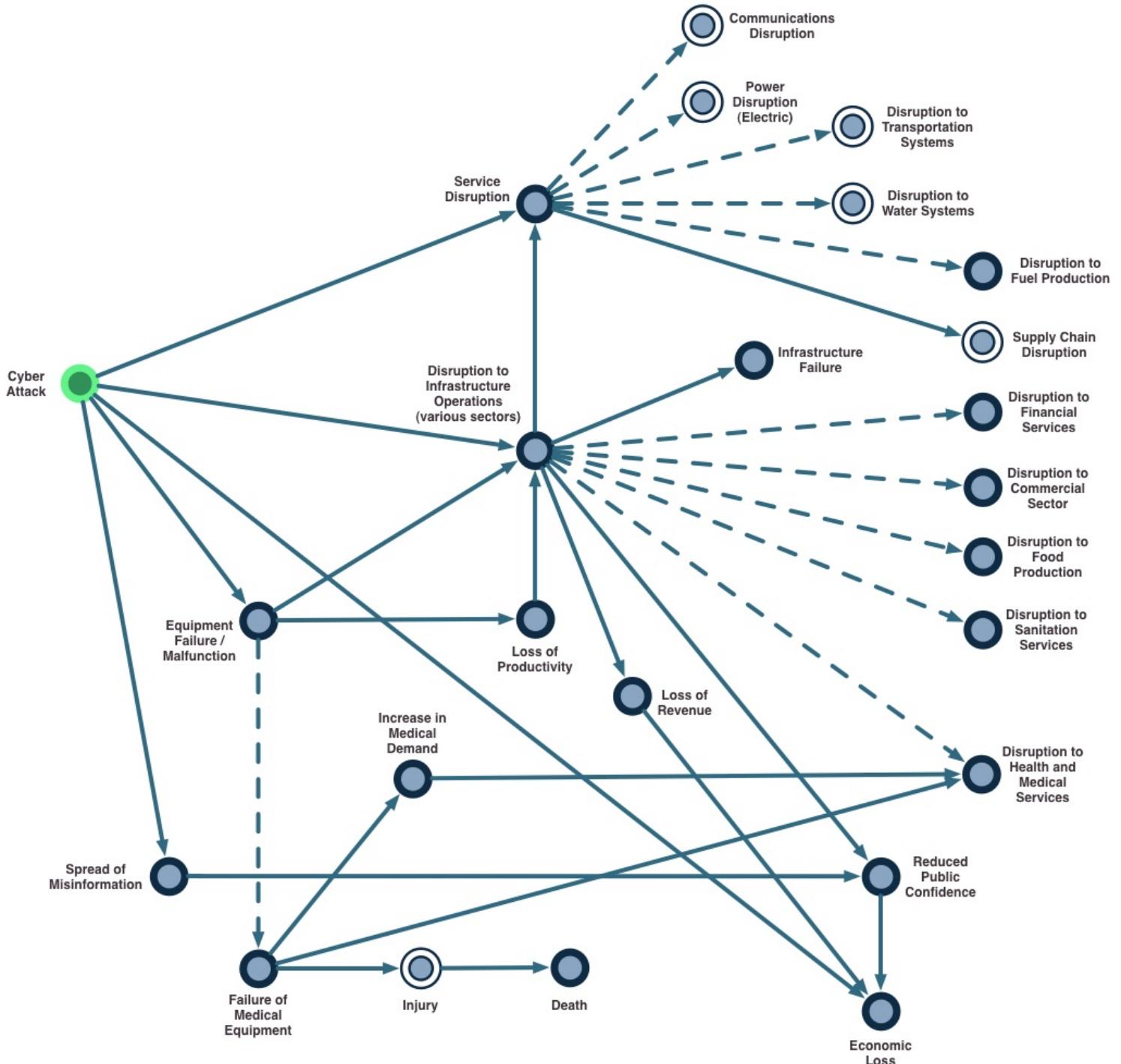


Z.6. CYBER ATTACK

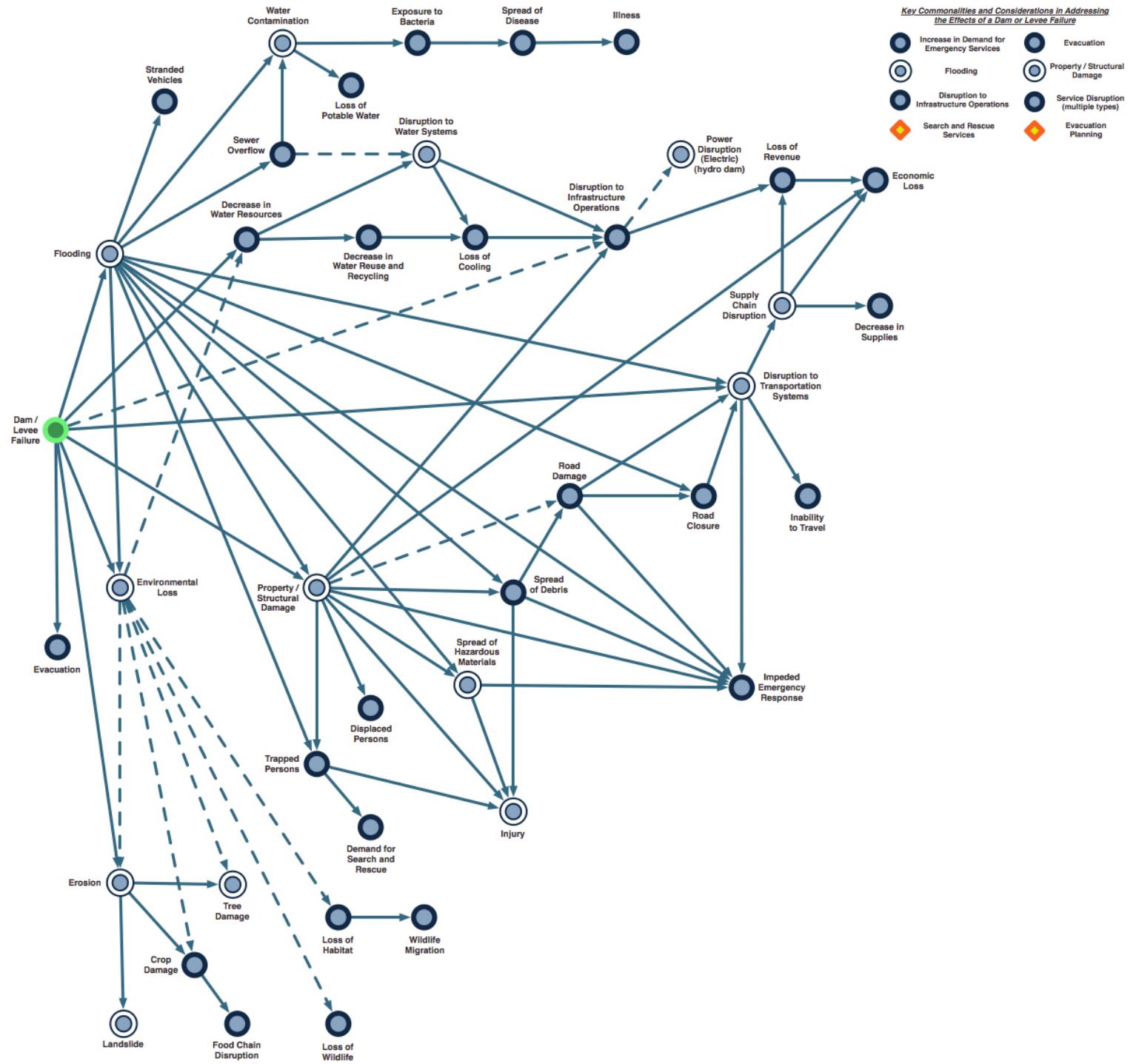
The following is a systematic approach to a Cyber Attack. A [Glossary of Cyber Terminology](#) is provided at the end of this Appendix.



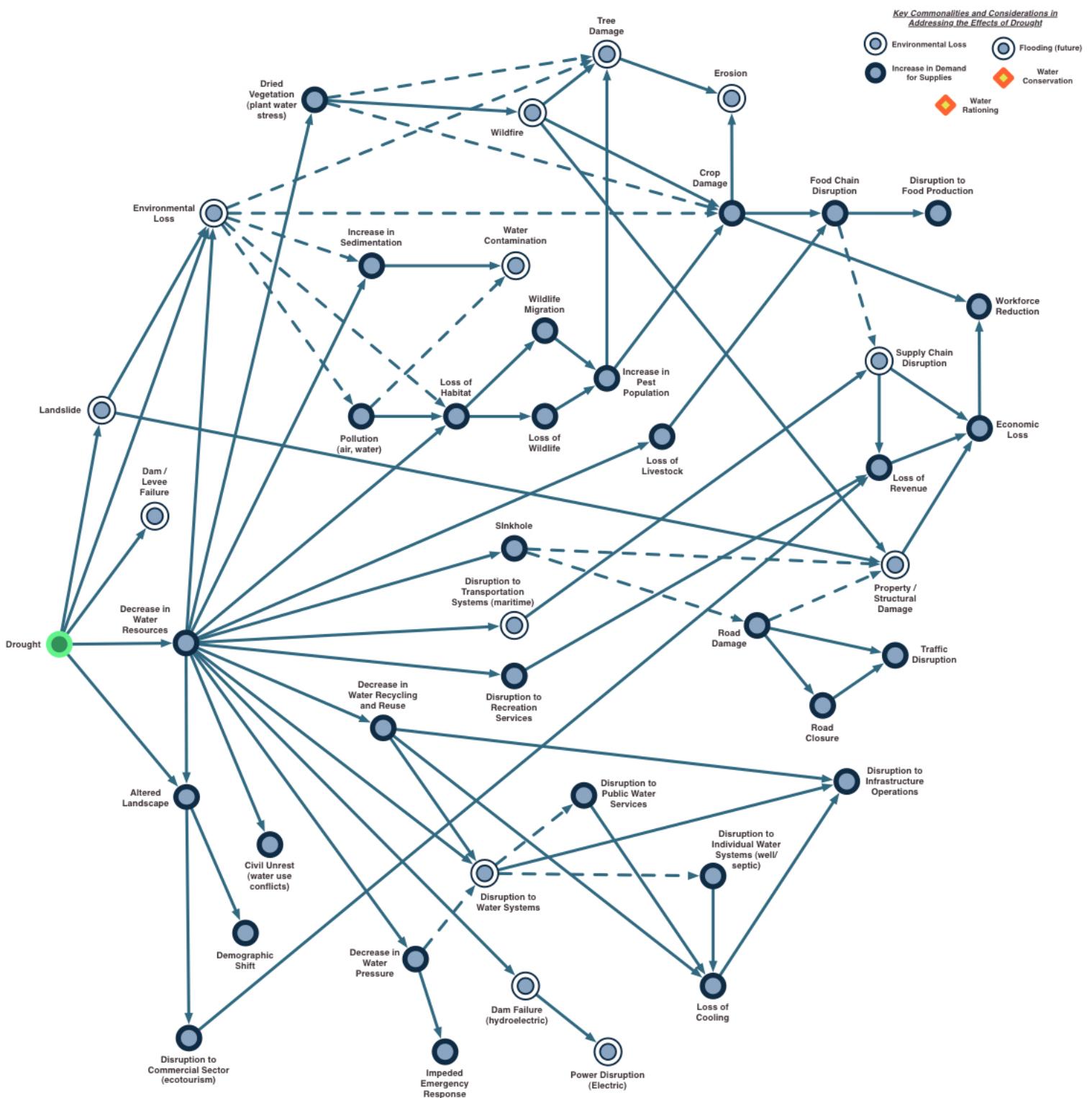
A Cyber Attack may result in numerous consequences (impacts) dependent on the target and scope of the attack. Information on additional cascading effects of a Cyber Attack is available on the various hazard networks within this section, chiefly those related to specific infrastructure sectors.



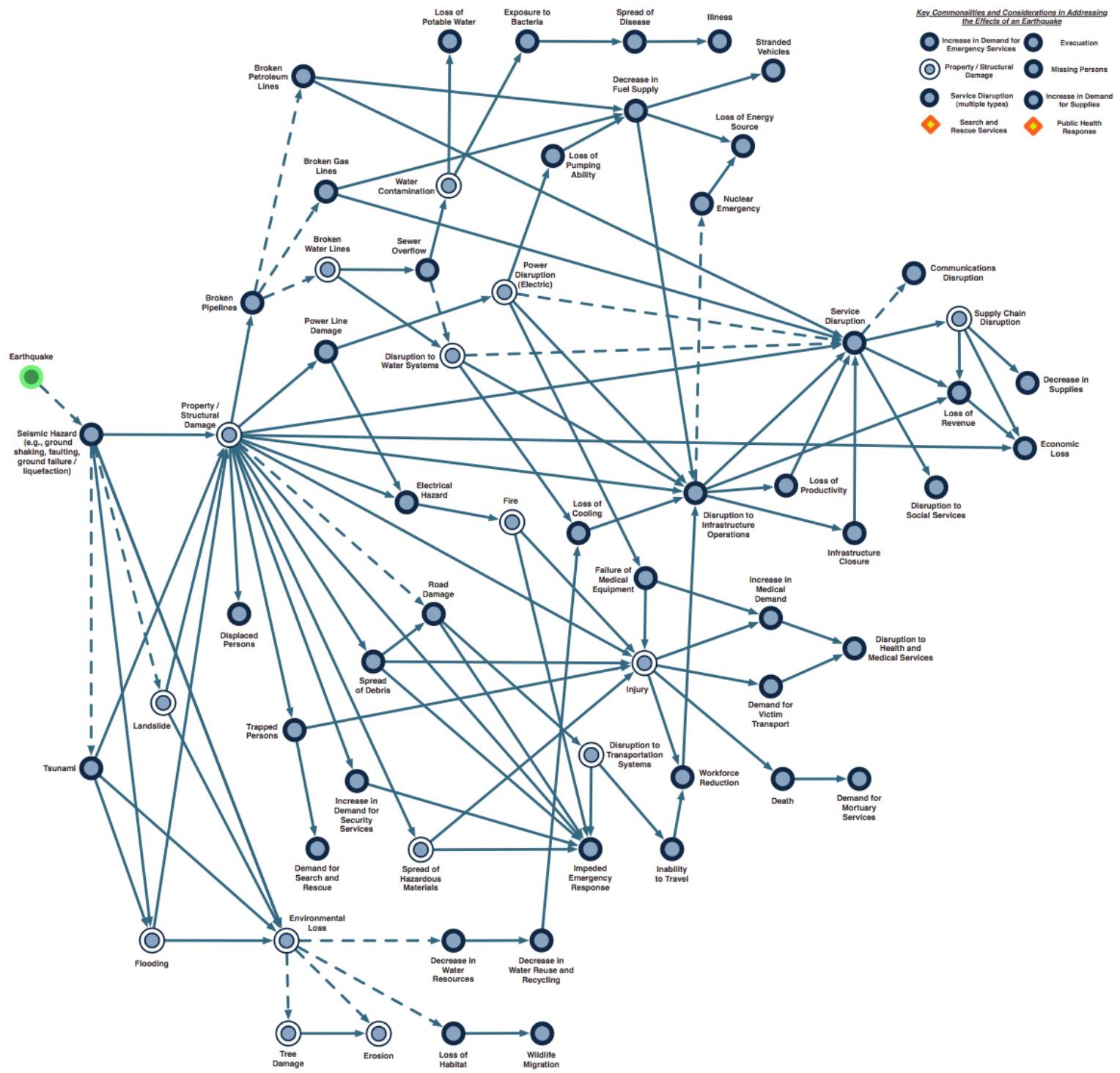
Z.7. DAM/LEVEE FAILURE



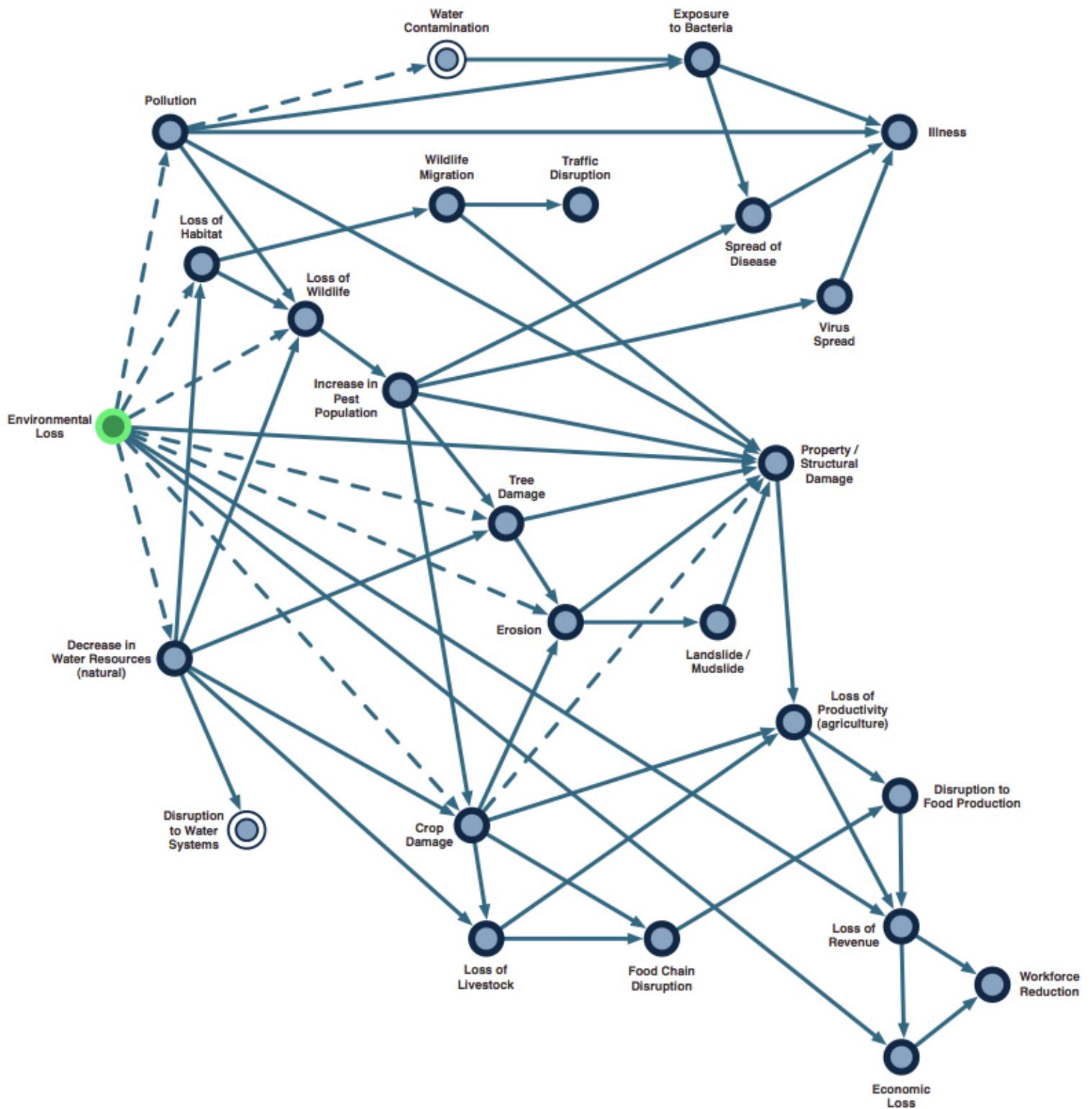
Z.8. DROUGHT



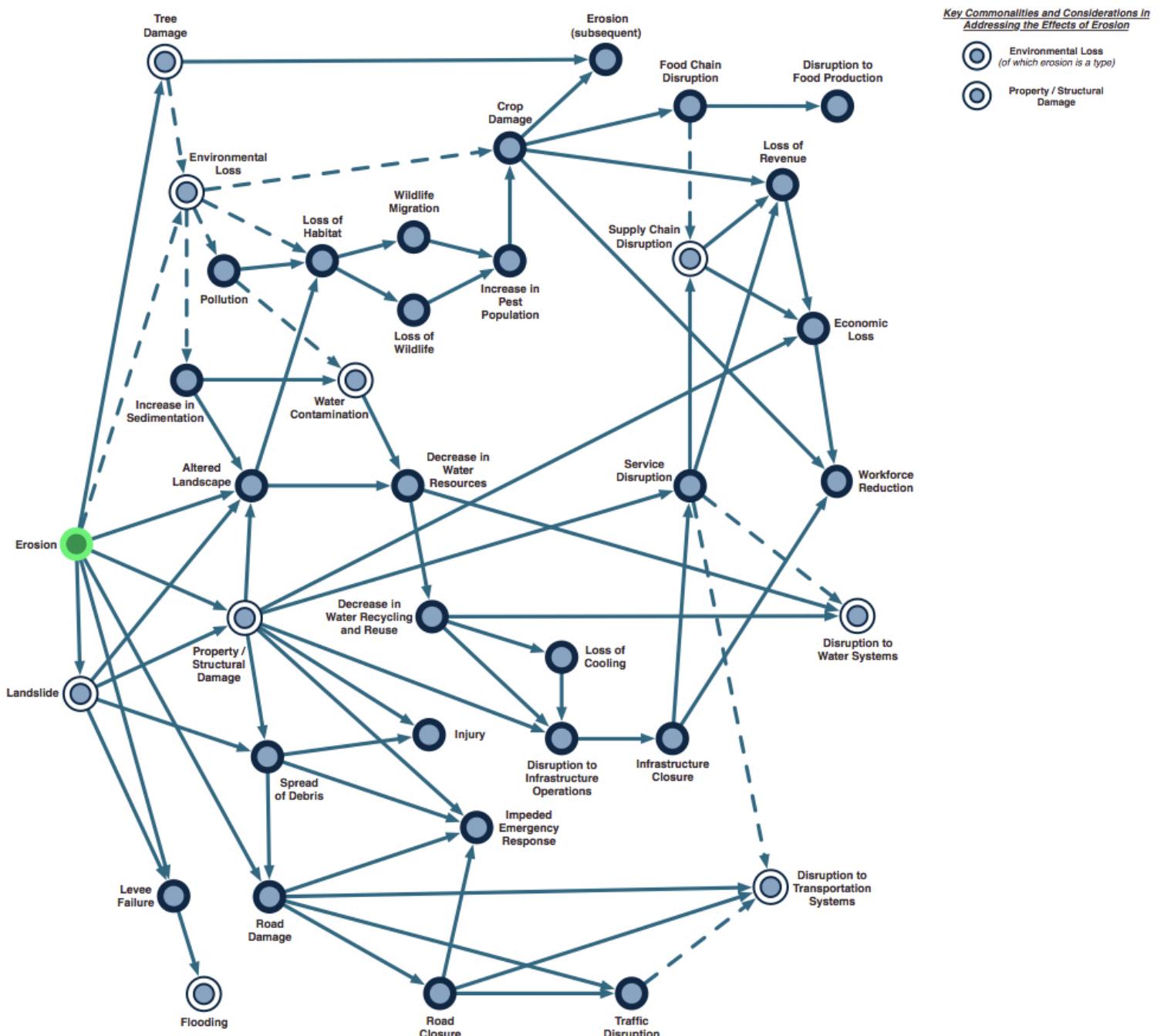
Z.9. EARTHQUAKE



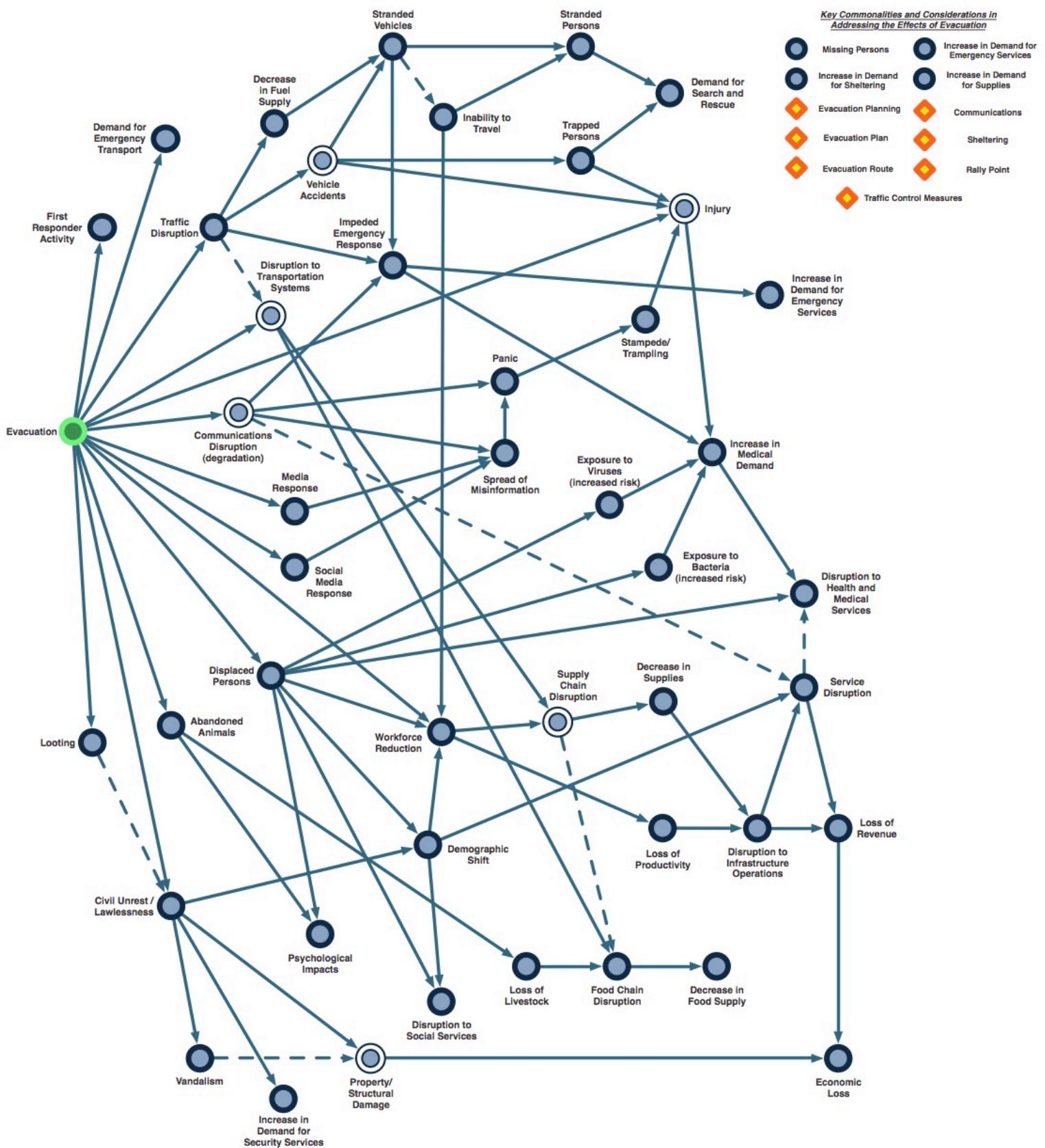
Z.10. ENVIRONMENTAL LOSS



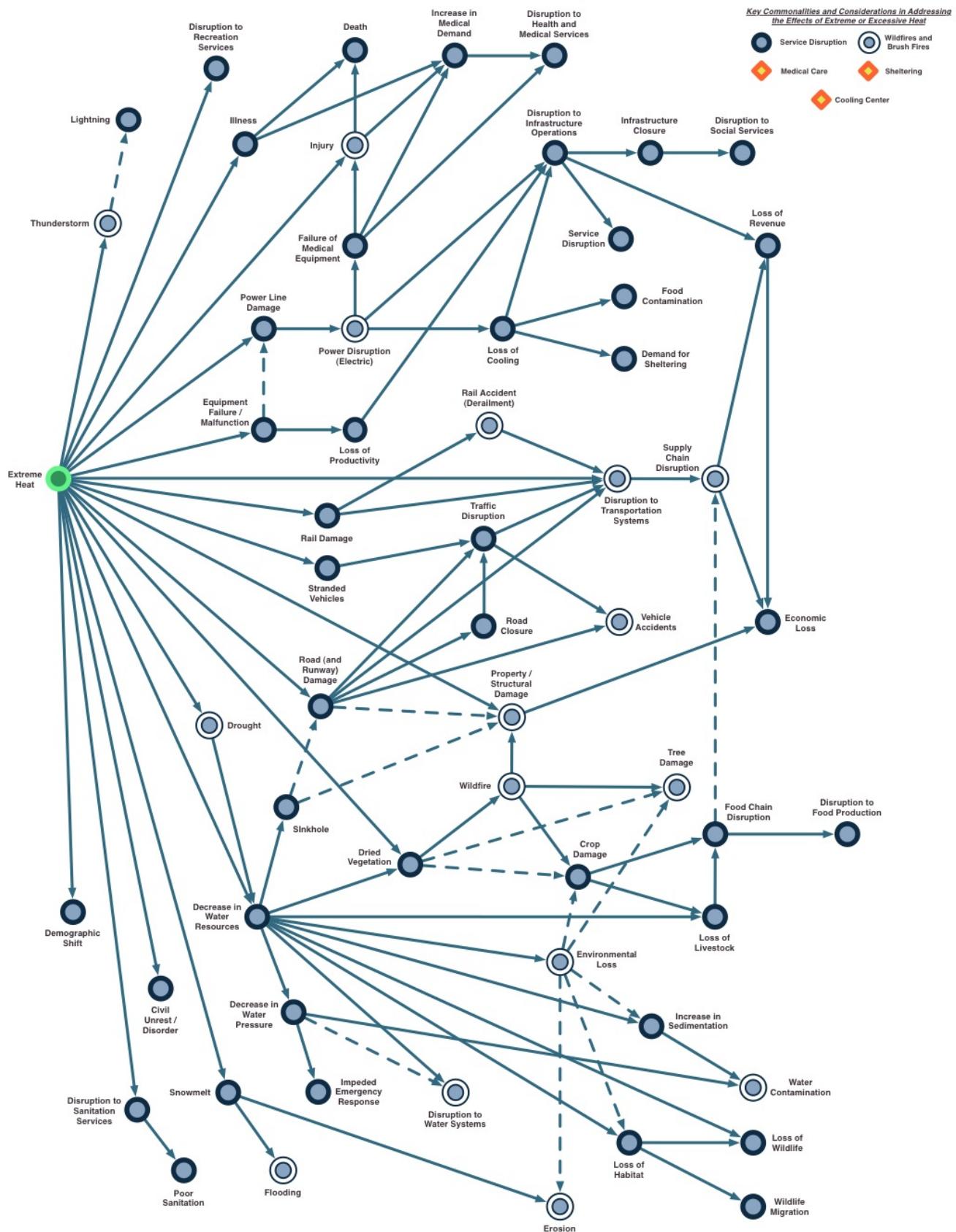
Z.11. EROSION



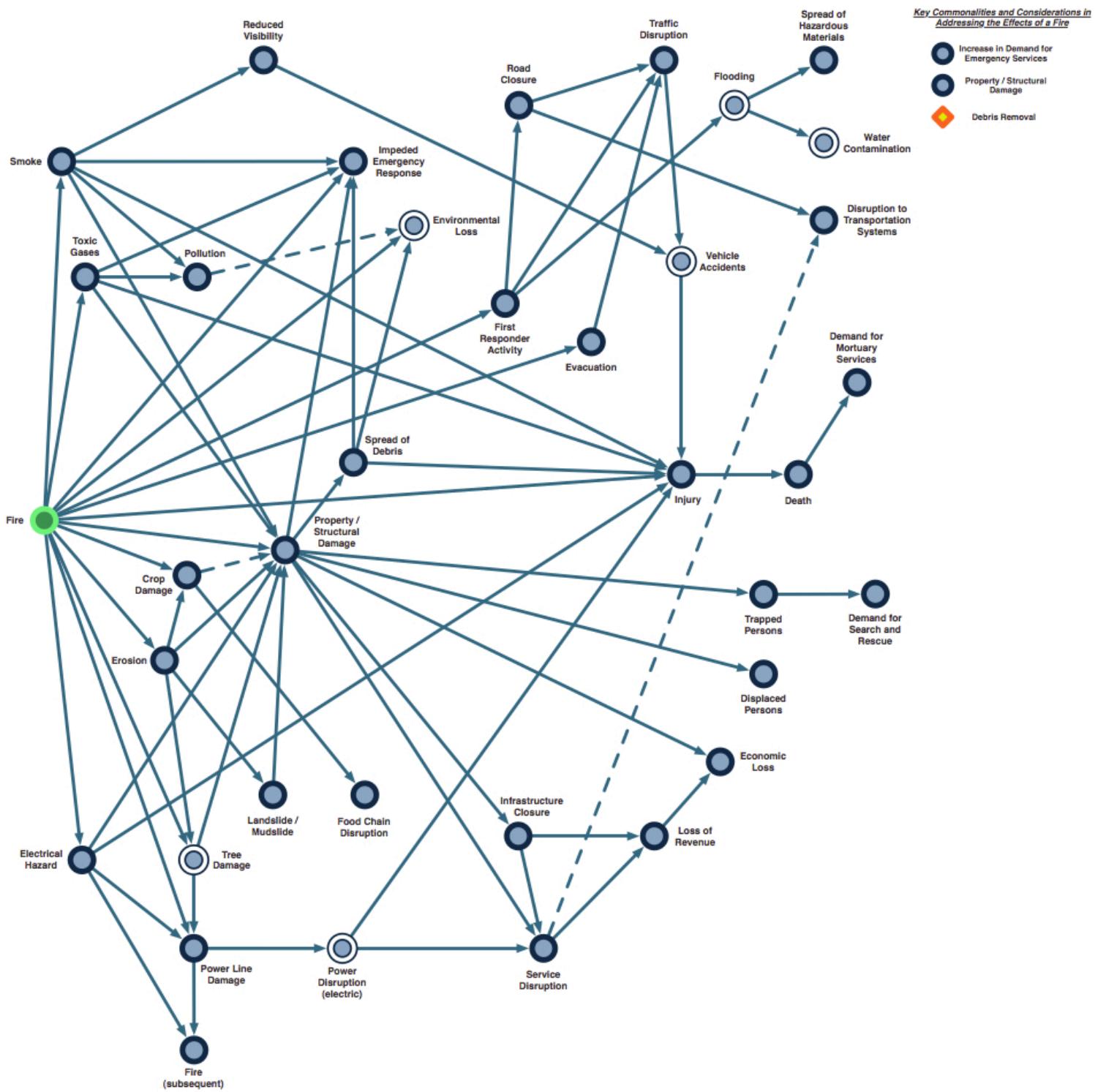
Z.12. EVACUATION



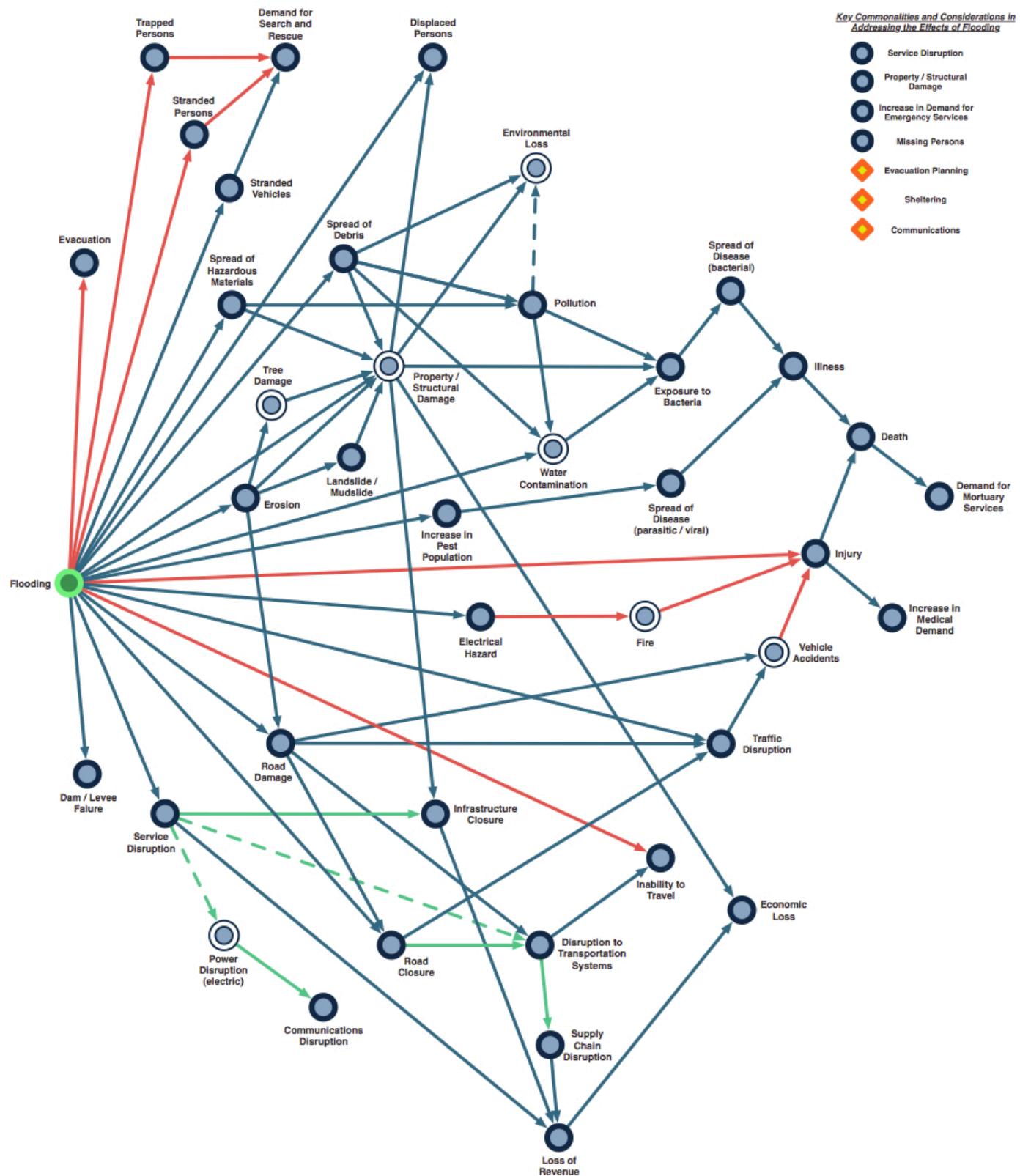
Z.13. EXTREME HEAT



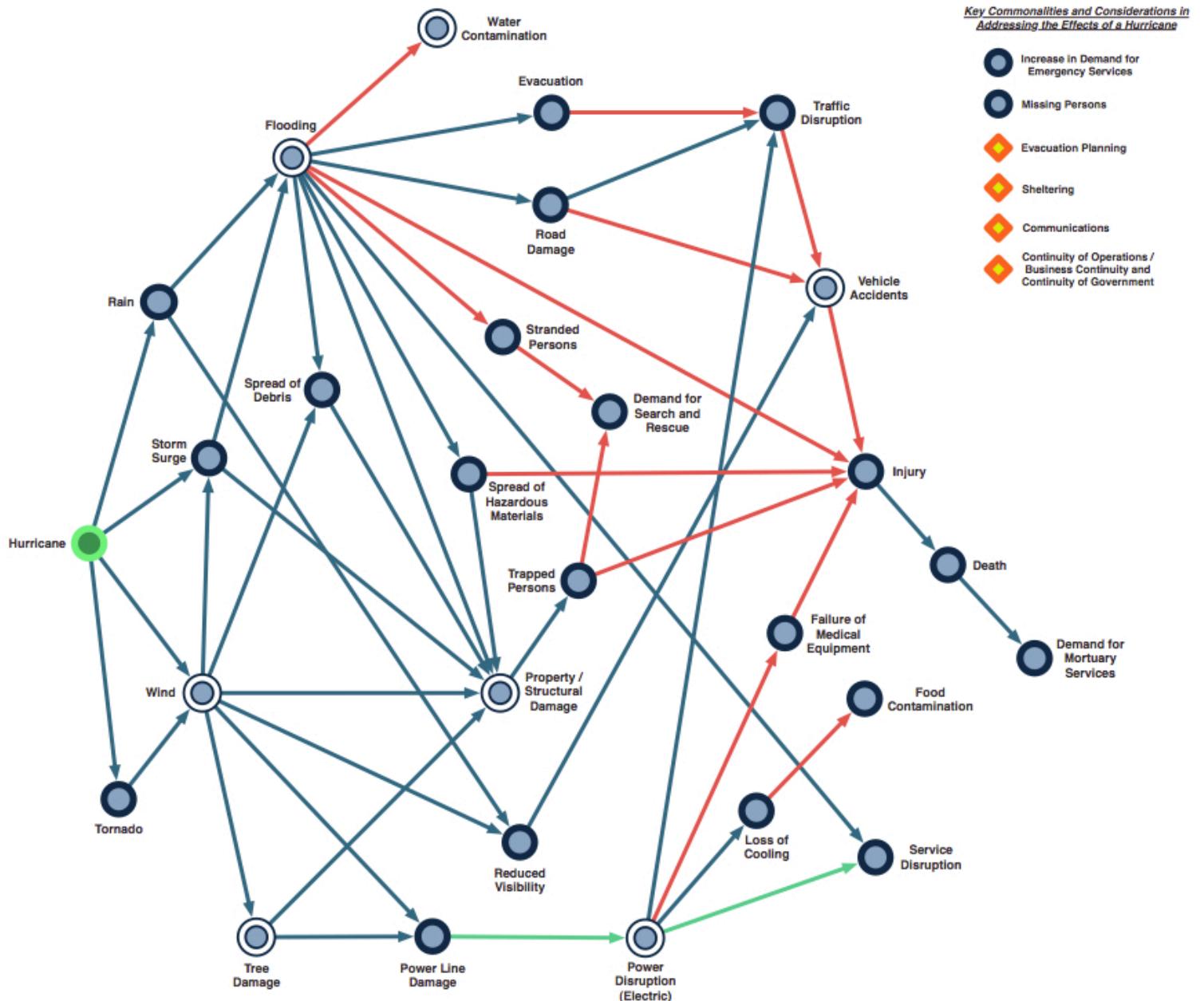
Z.14. FIRE



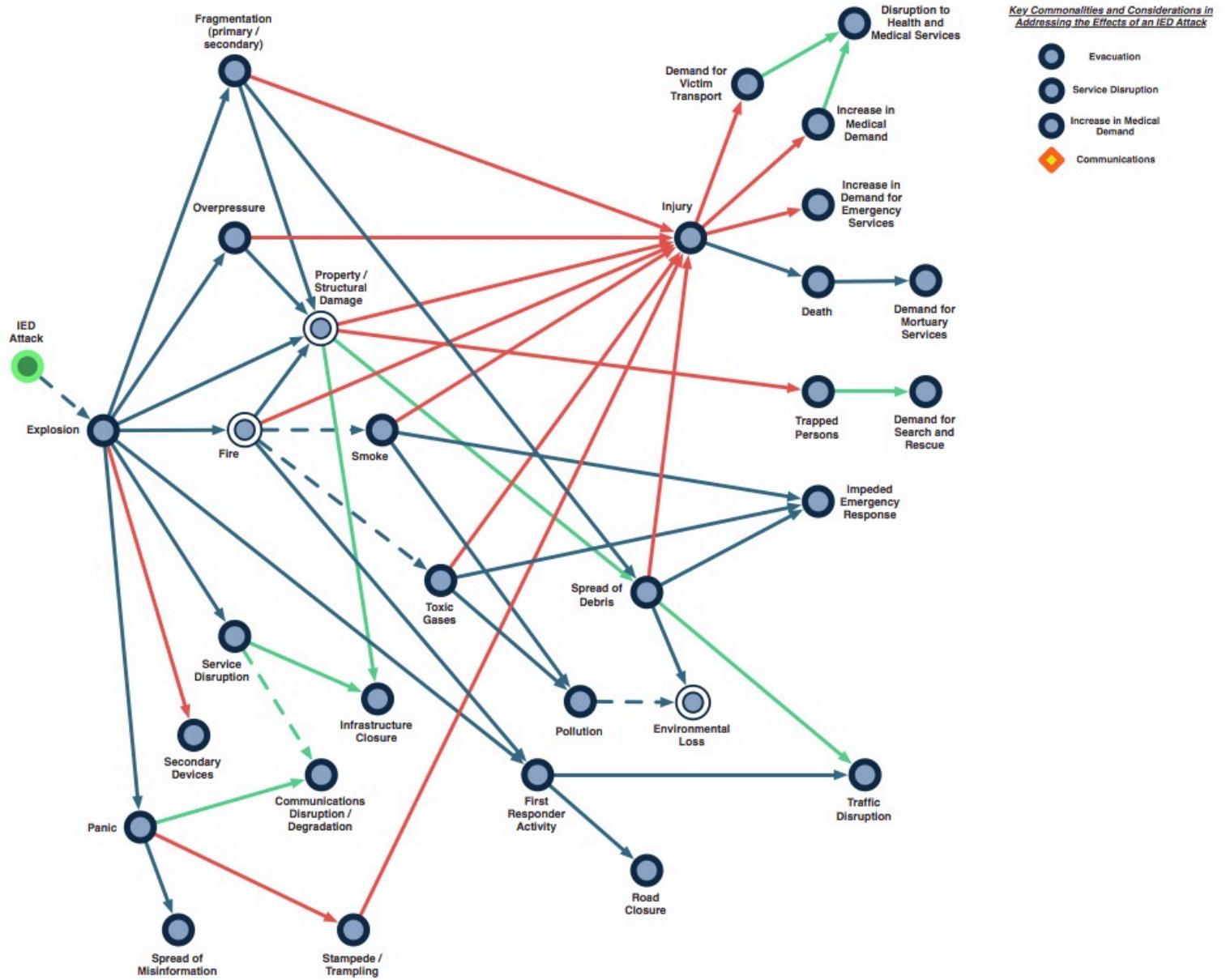
Z.15. FLOODING



Z.16. HURRICANE

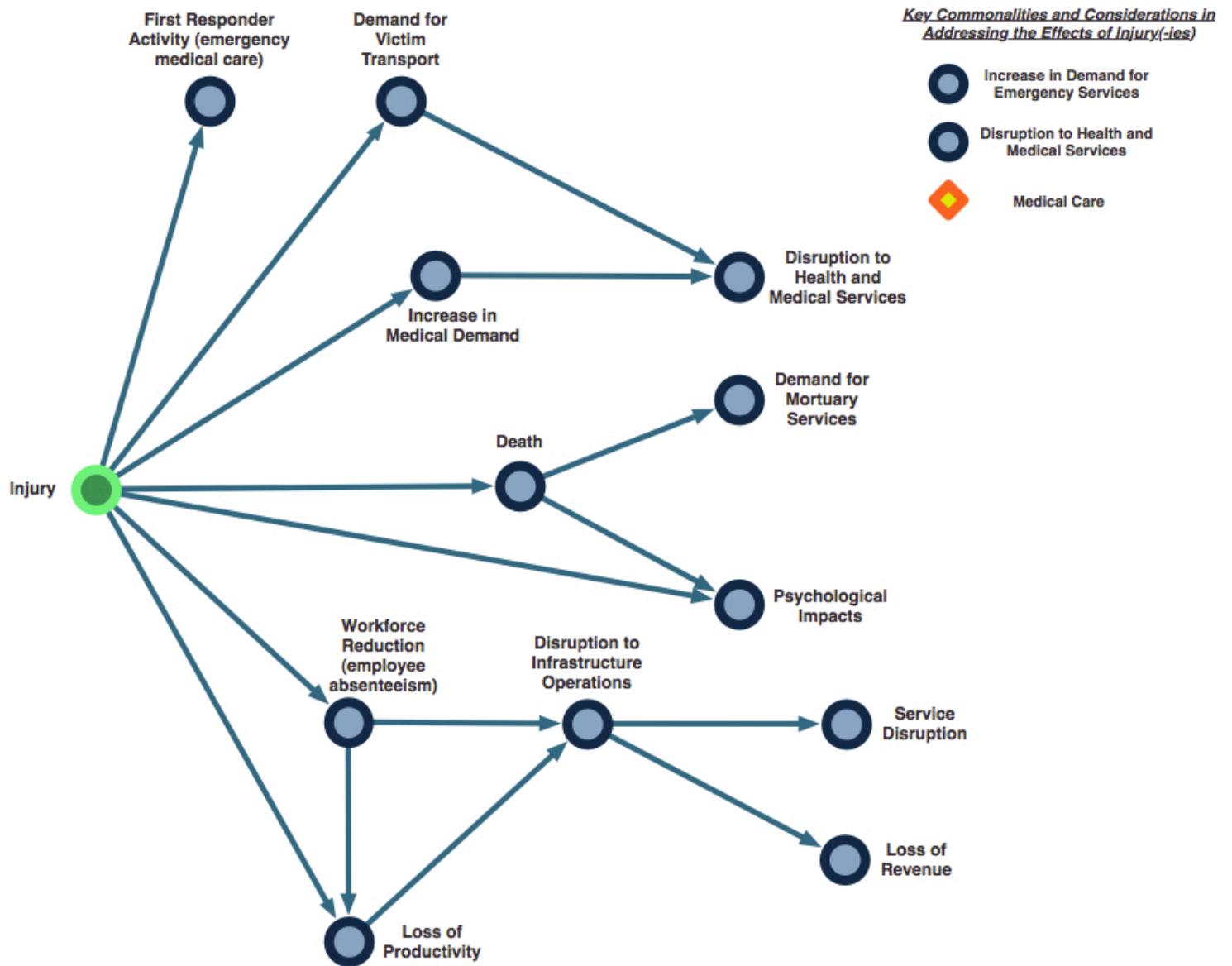


Z.17. IMPROVISED EXPLOSIVE DEVICE

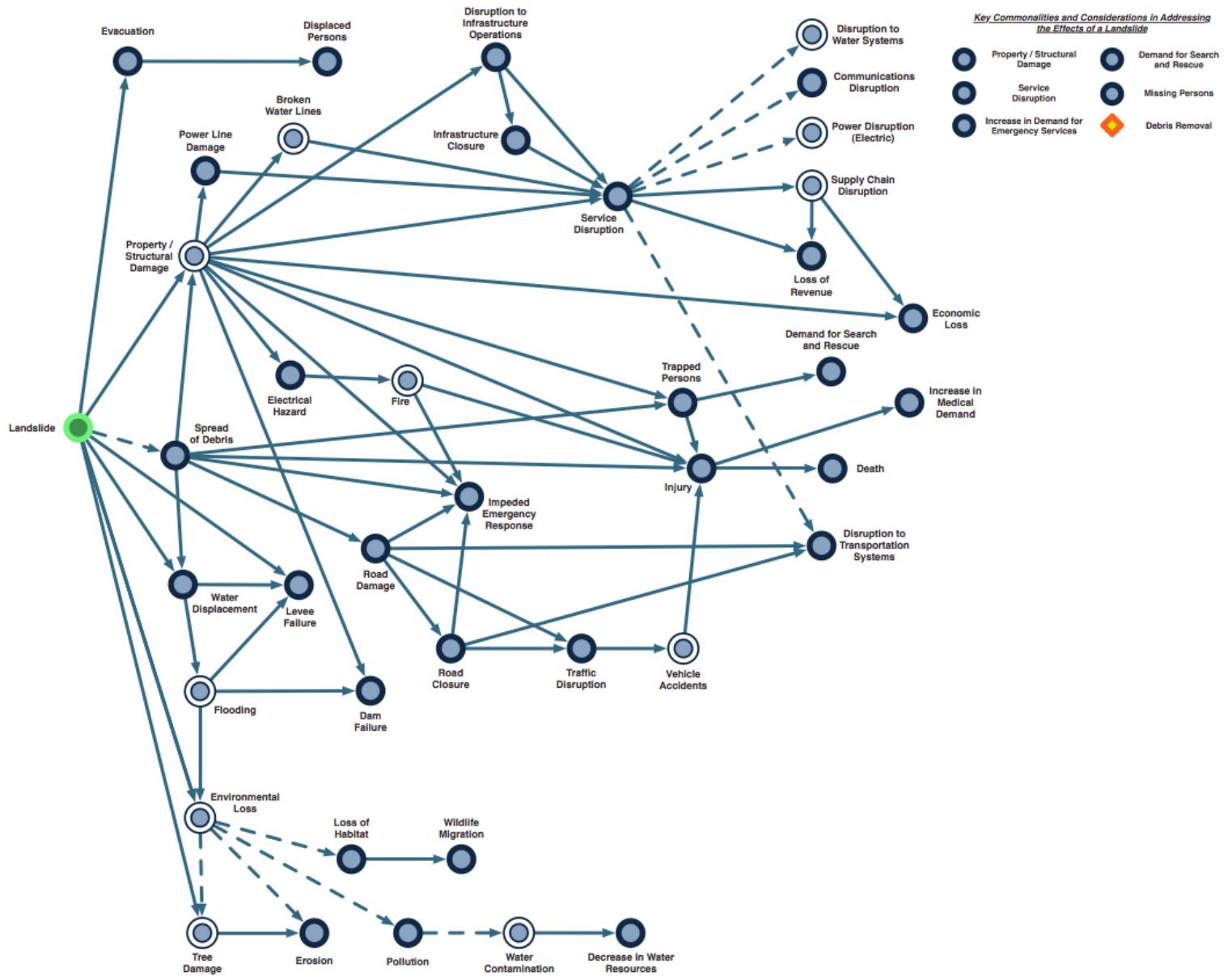


Z.18. INJURY

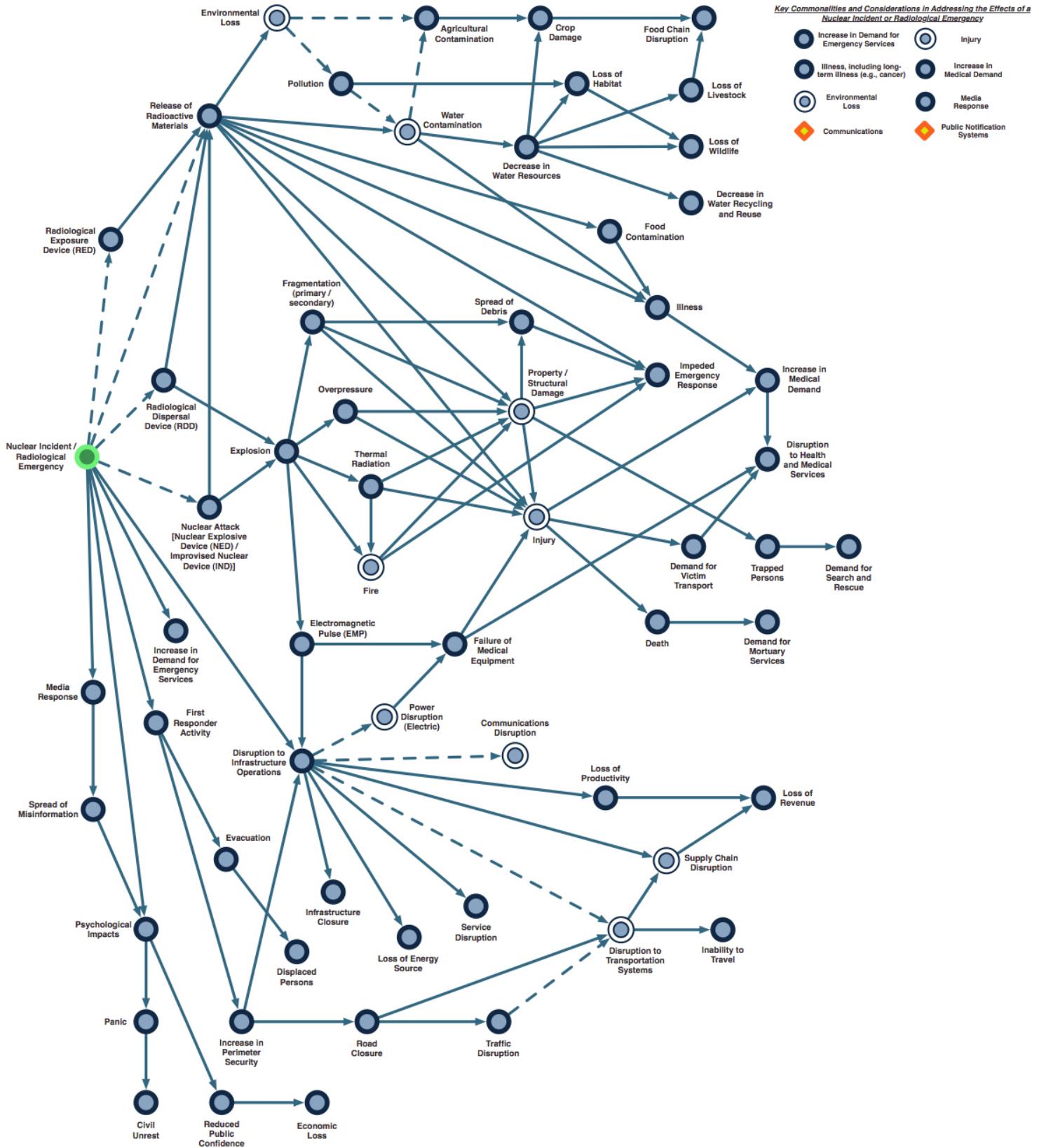
The below hazard network is also relevant to illness.



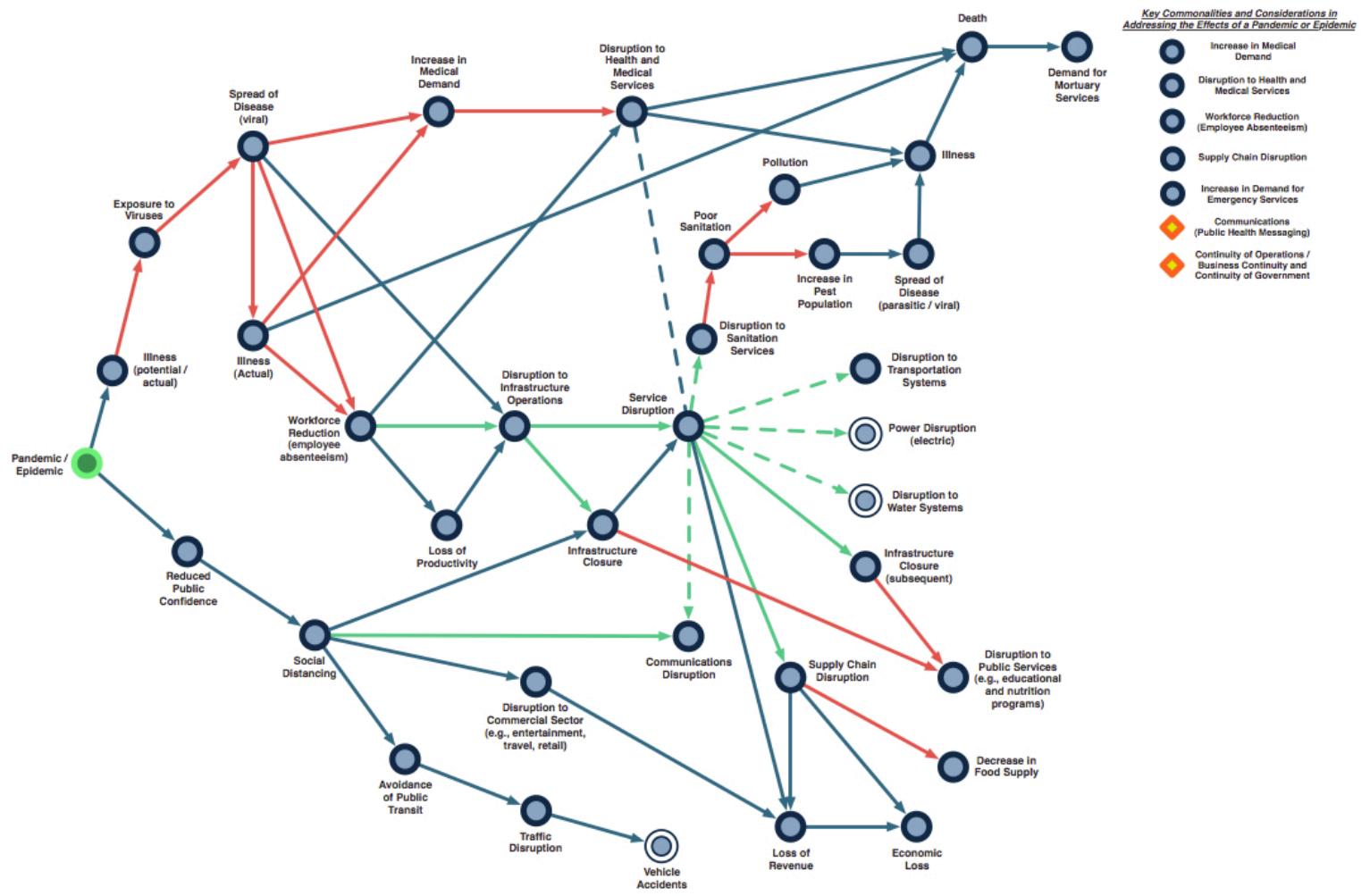
Z.19. LANDSLIDE



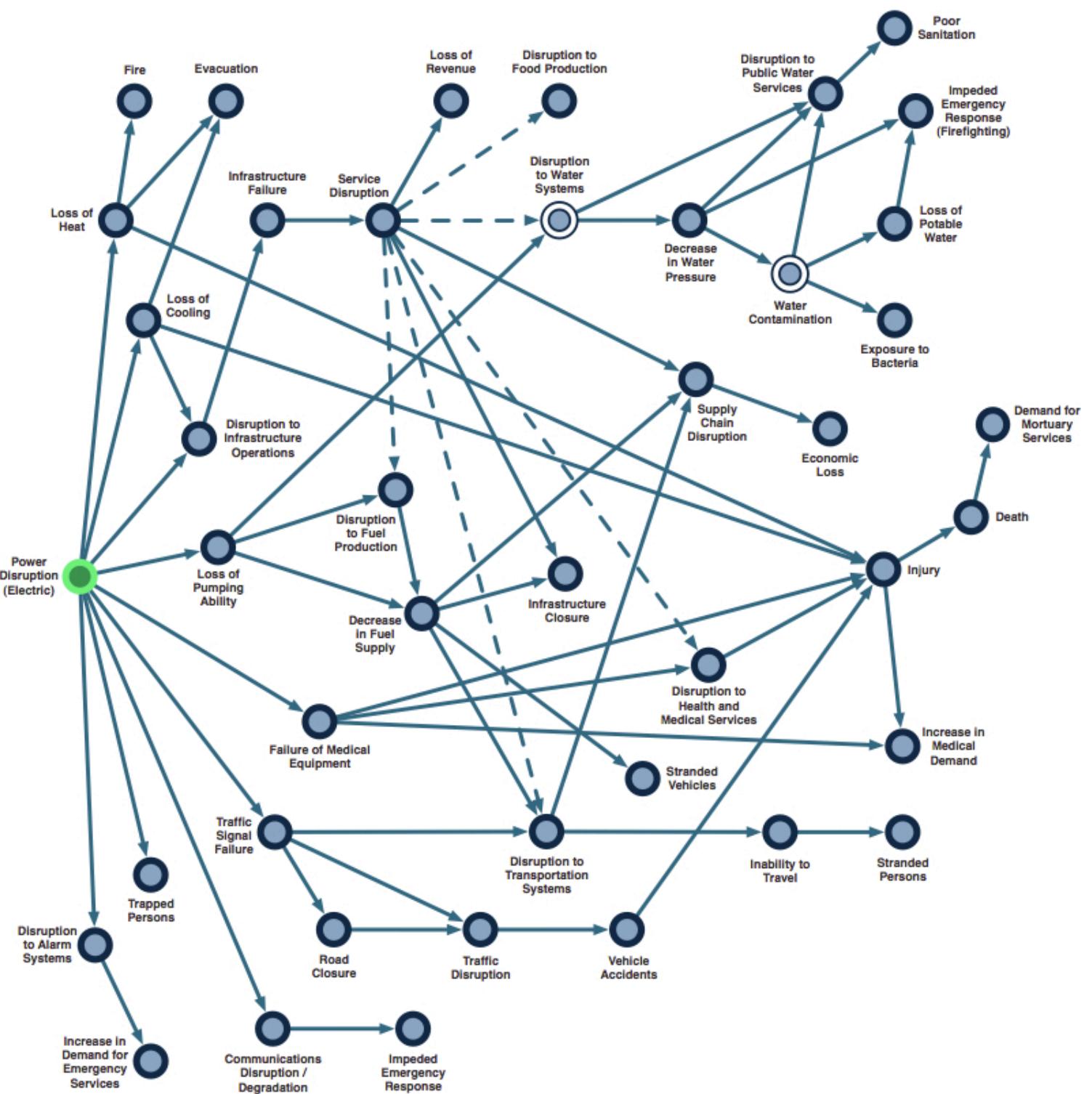
Z.20. NUCLEAR INCIDENT / RADIological EMERGENCY



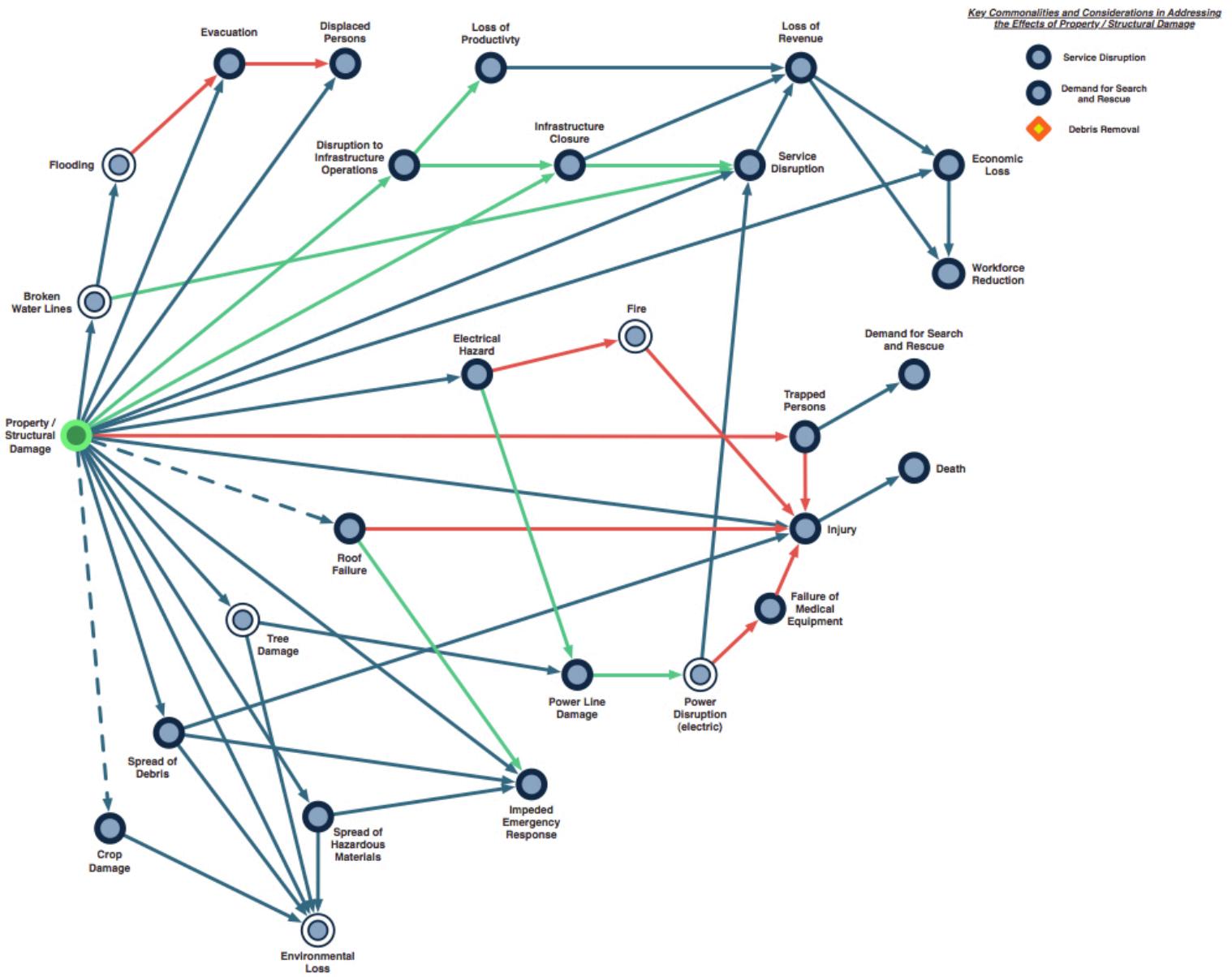
Z.21. PANDEMIC / EPIDEMIC



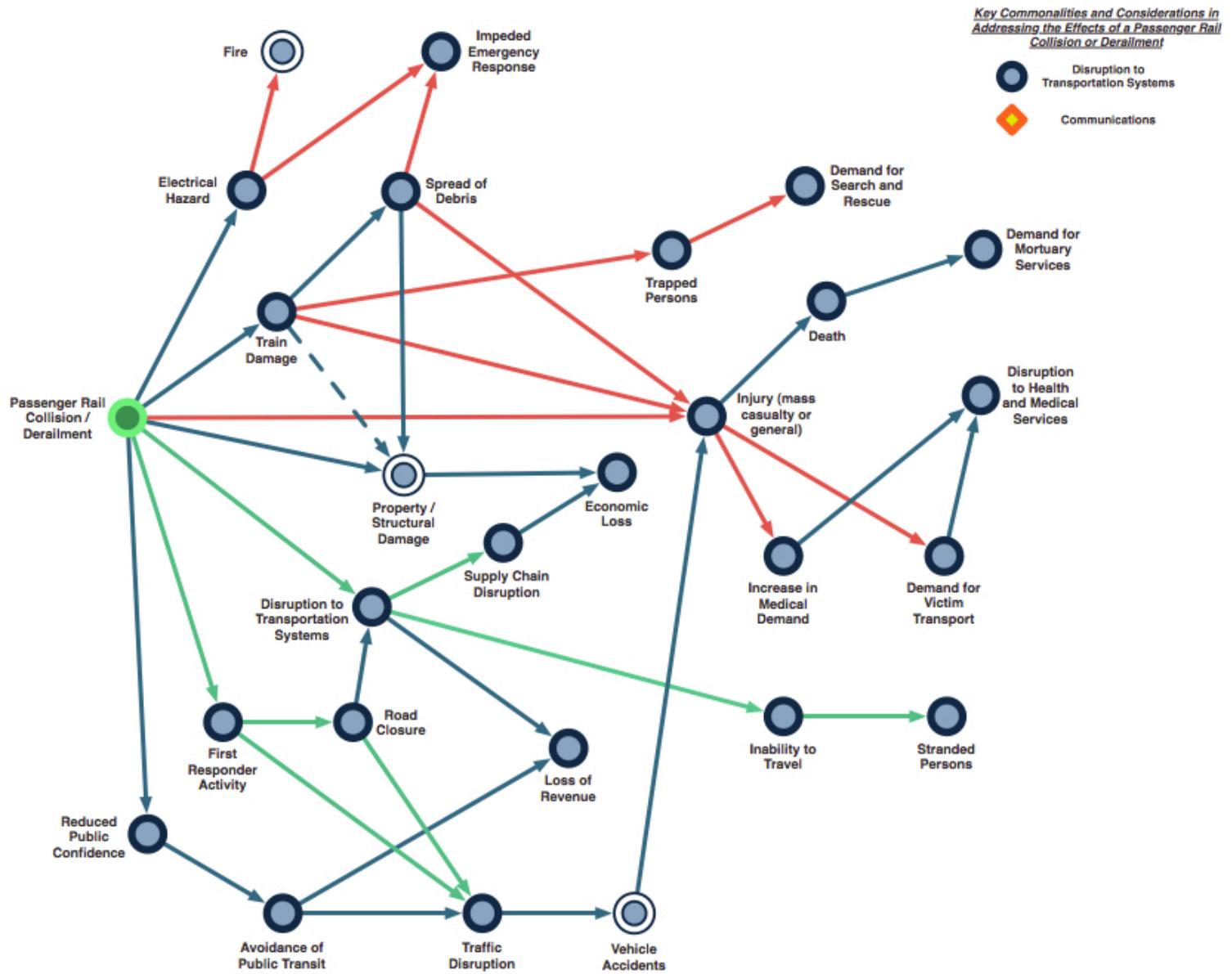
Z.22. POWER DISRUPTION (ELECTRIC)



Z.23. PROPERTY / STRUCTURAL DAMAGE

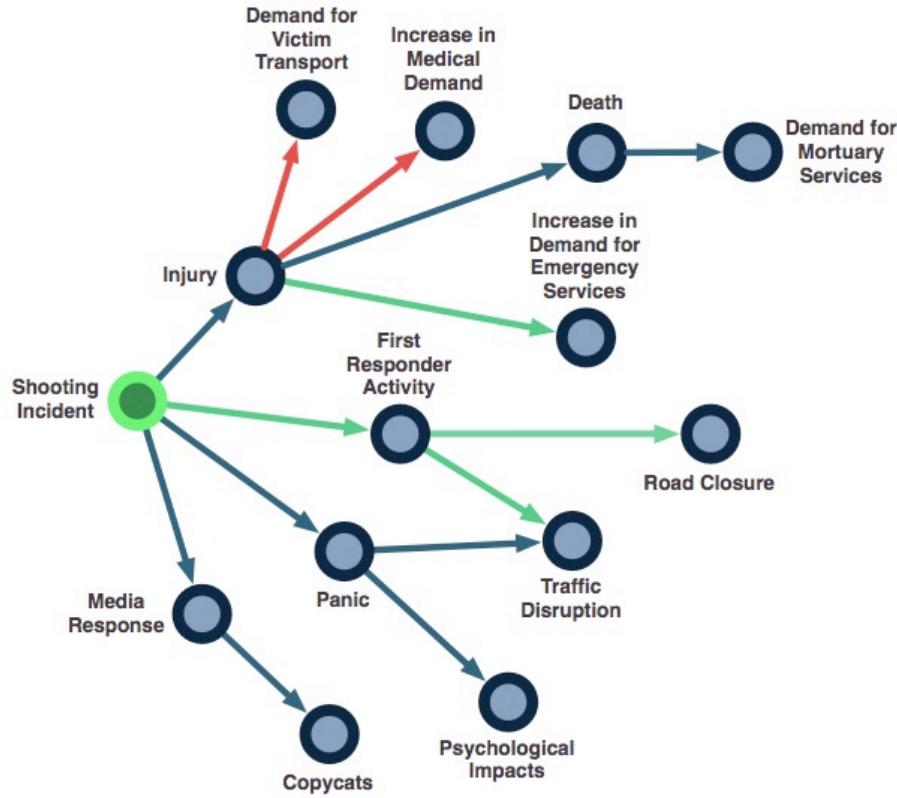


Z.24. PASSENGER RAIL COLLISION / DERAILMENT

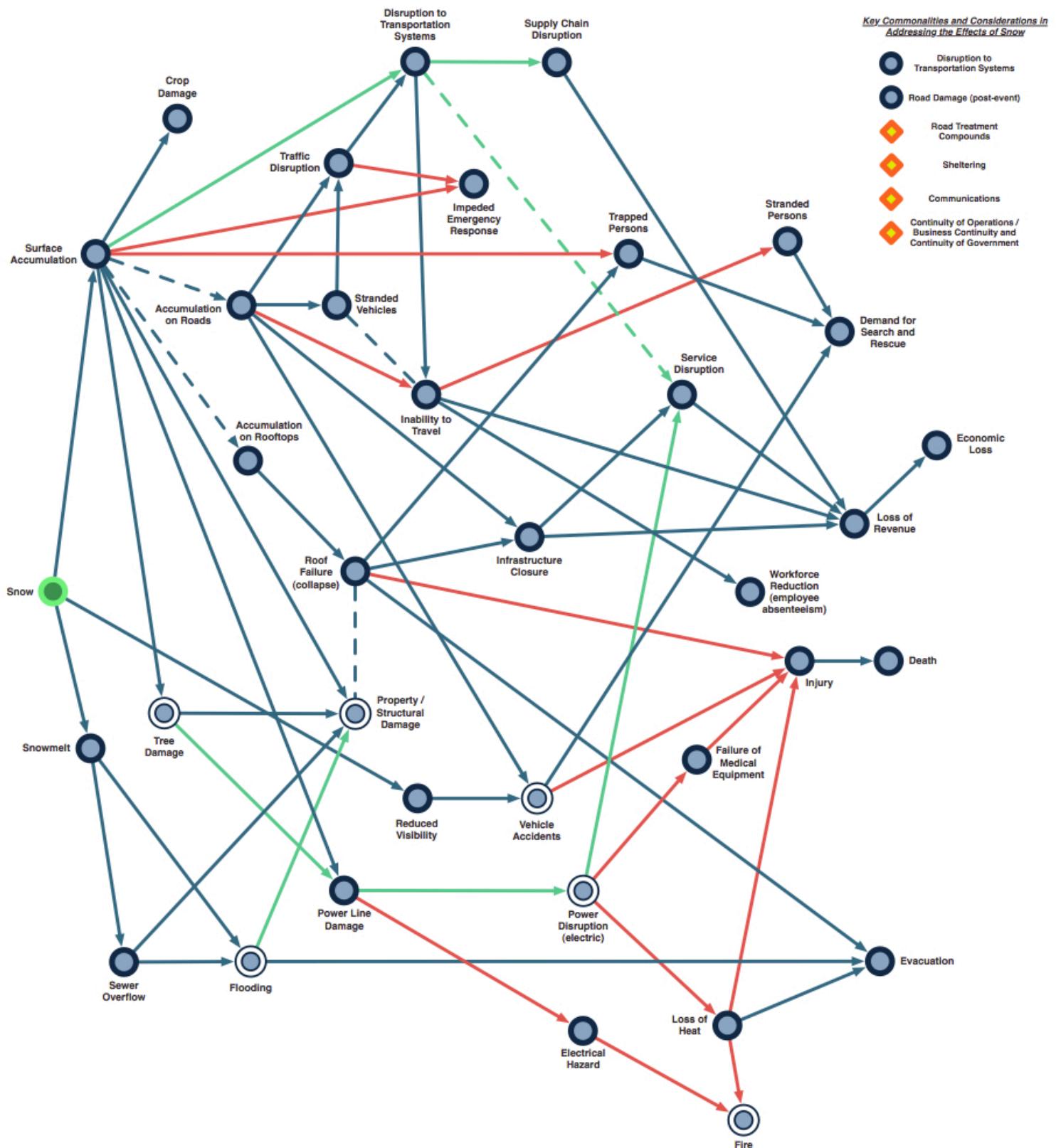


Z.25. SHOOTING INCIDENT

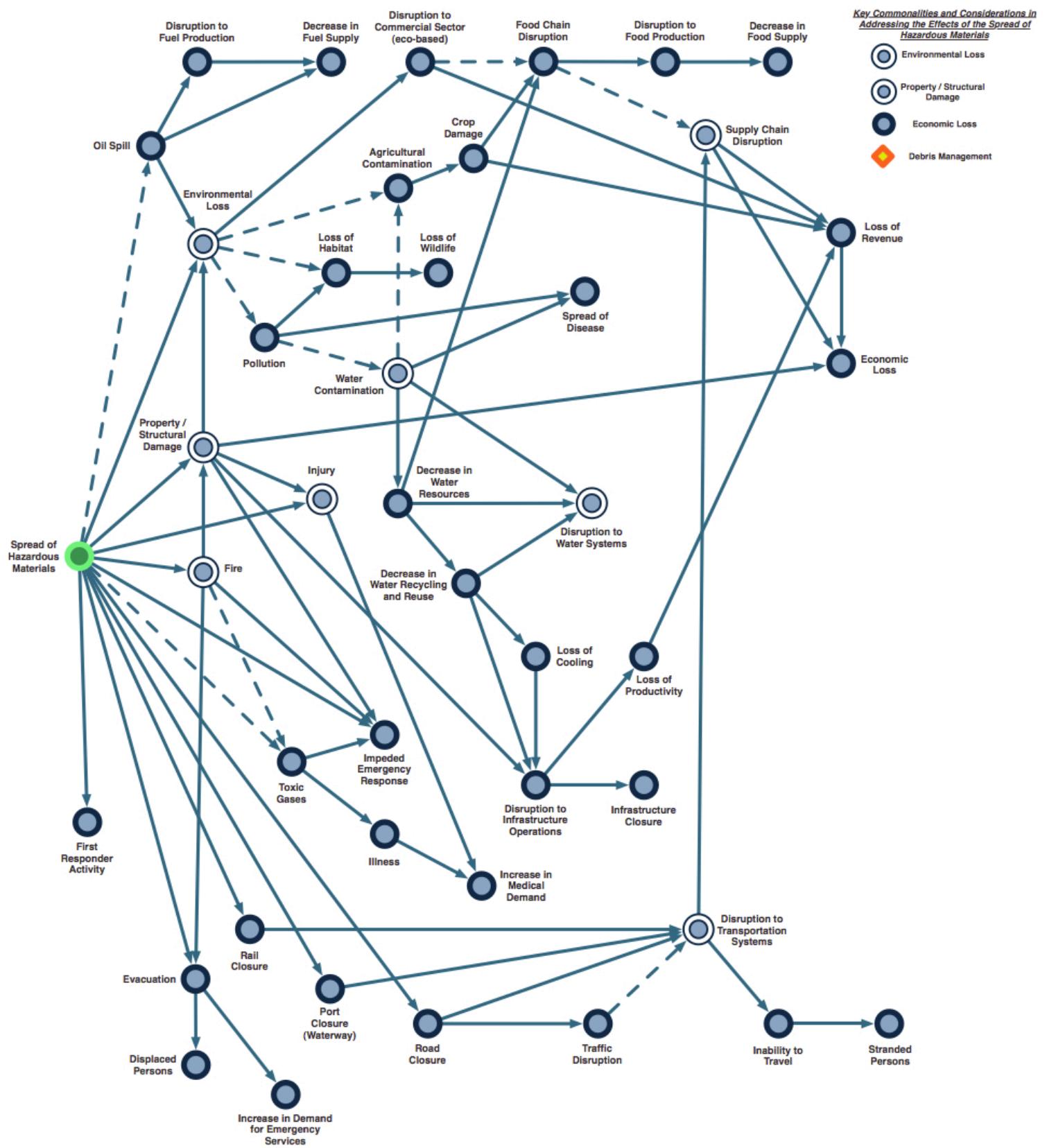
The below hazard network is a simple representation of the effects of a shooting incident; additional networks for certain cascading effects are available in this Appendix.



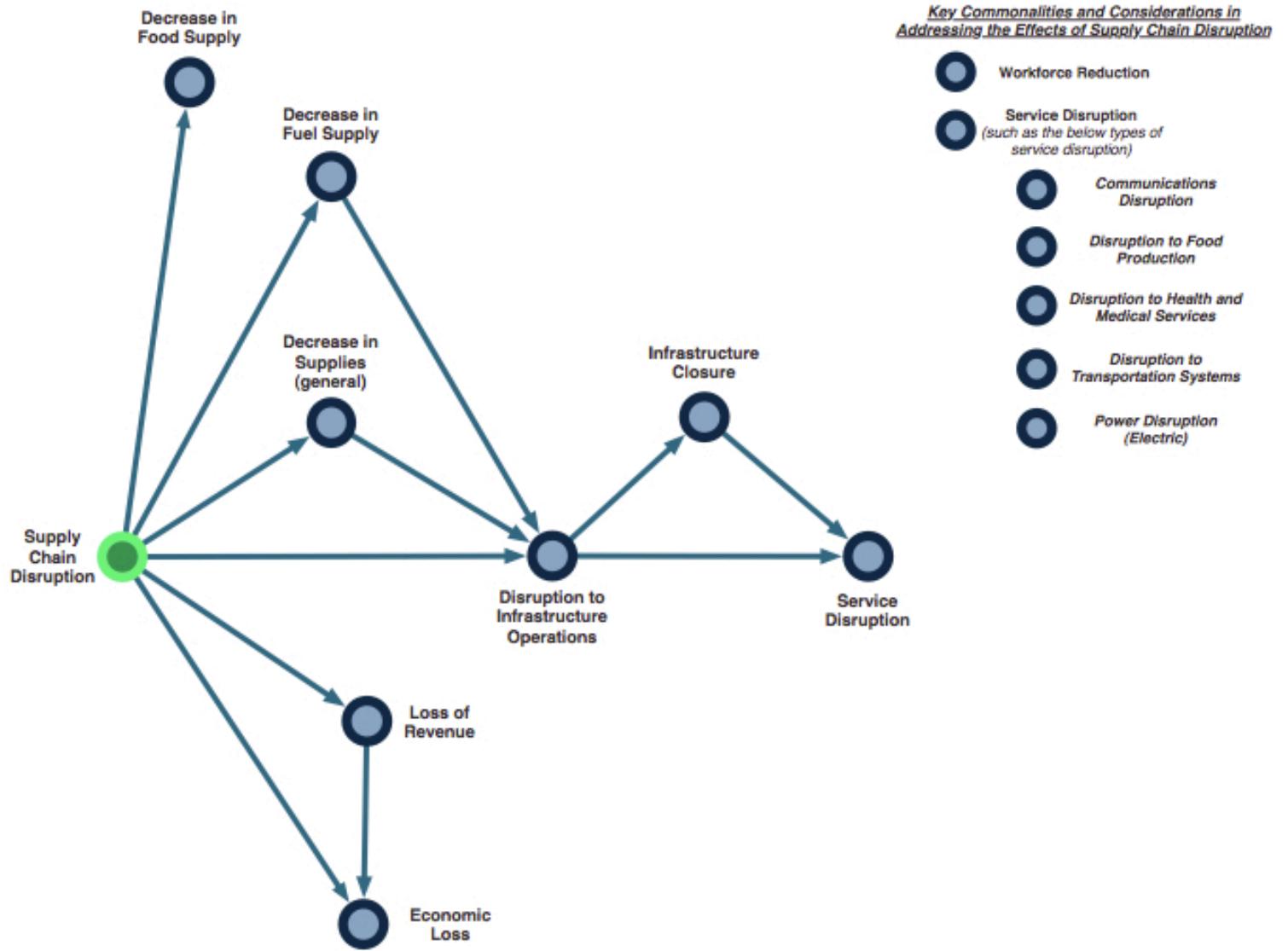
Z.26. SNOW



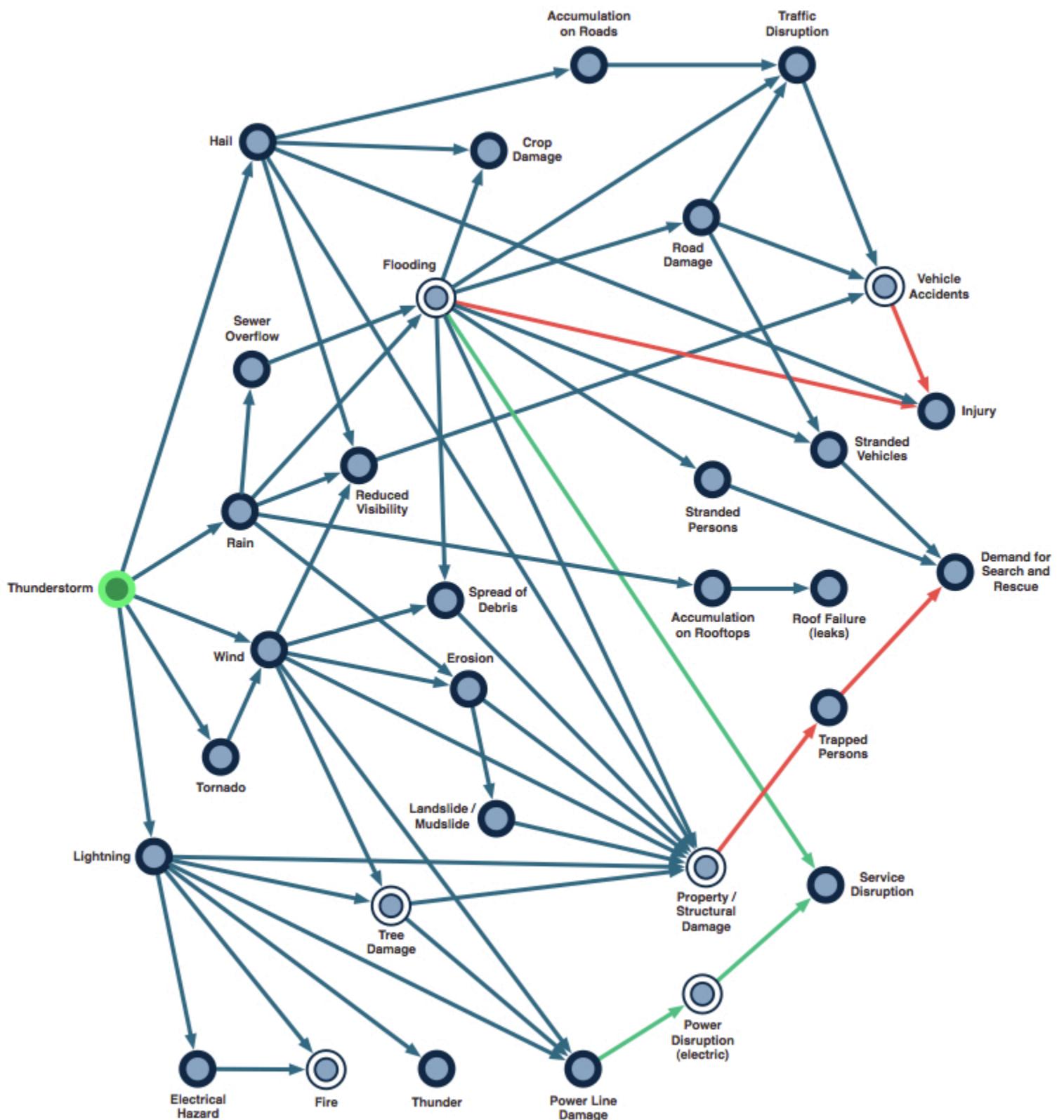
Z.27. SPREAD OF HAZARDOUS MATERIALS



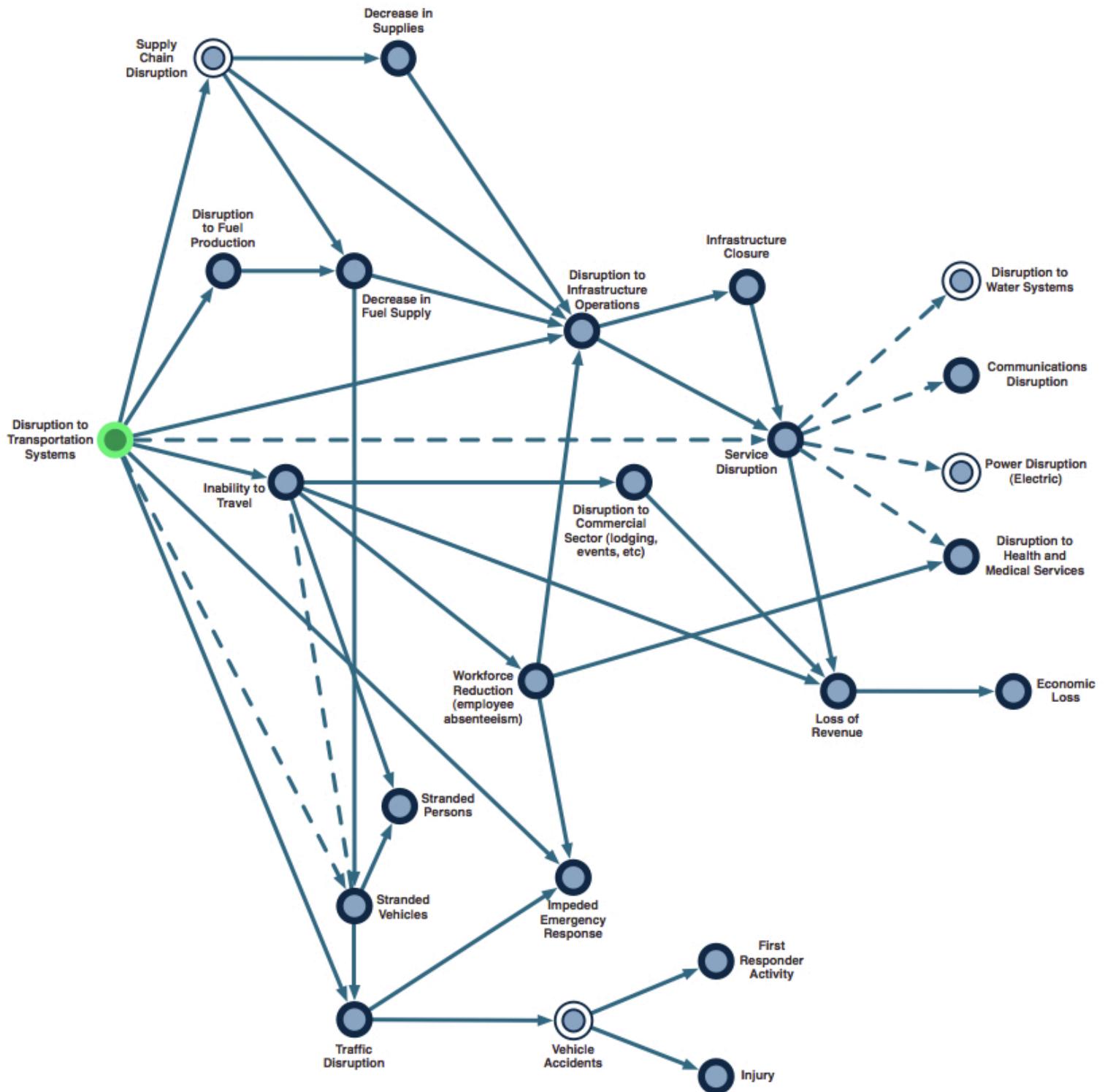
Z.28. SUPPLY CHAIN DISRUPTION



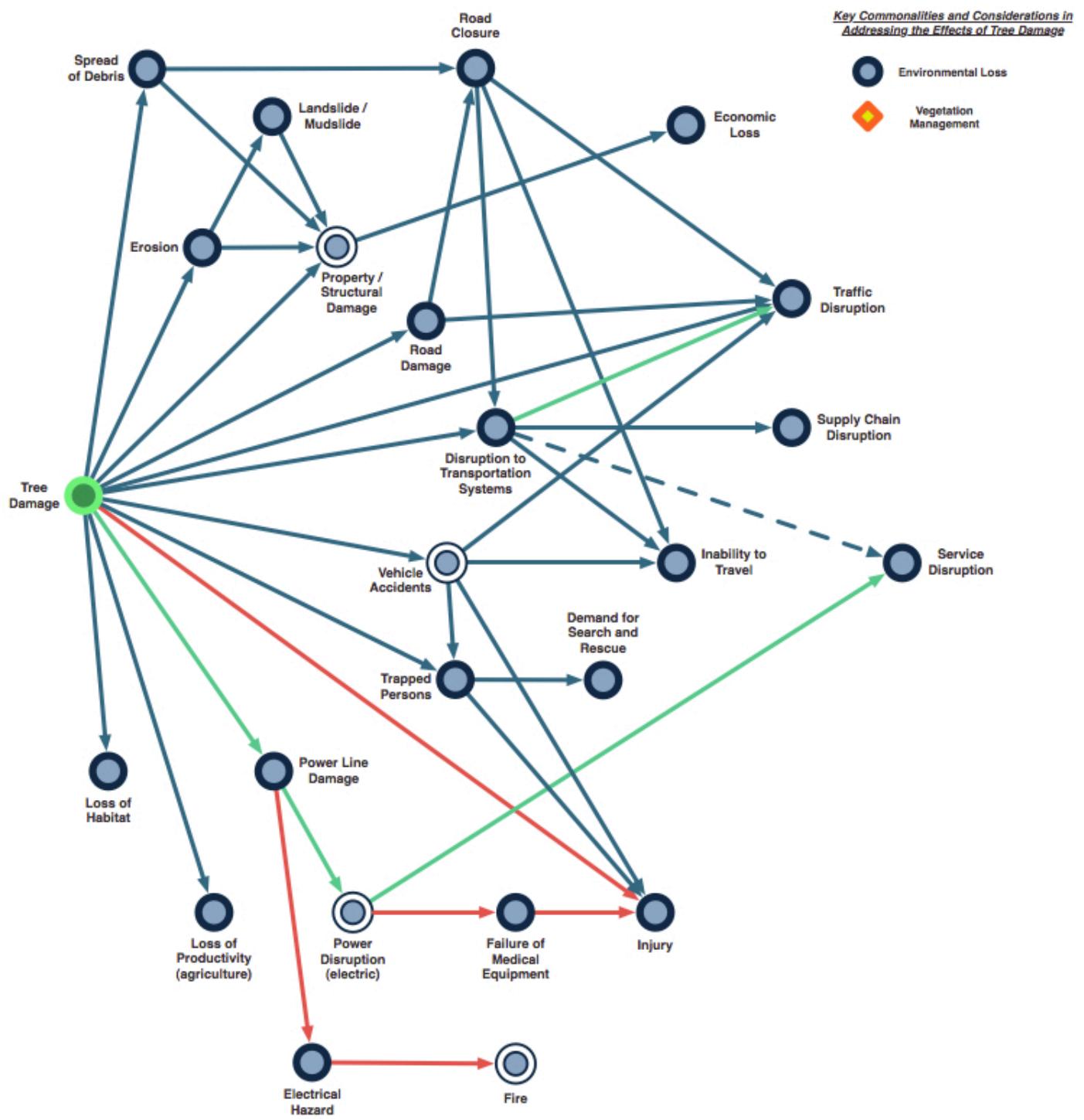
Z.29. THUNDERSTORM



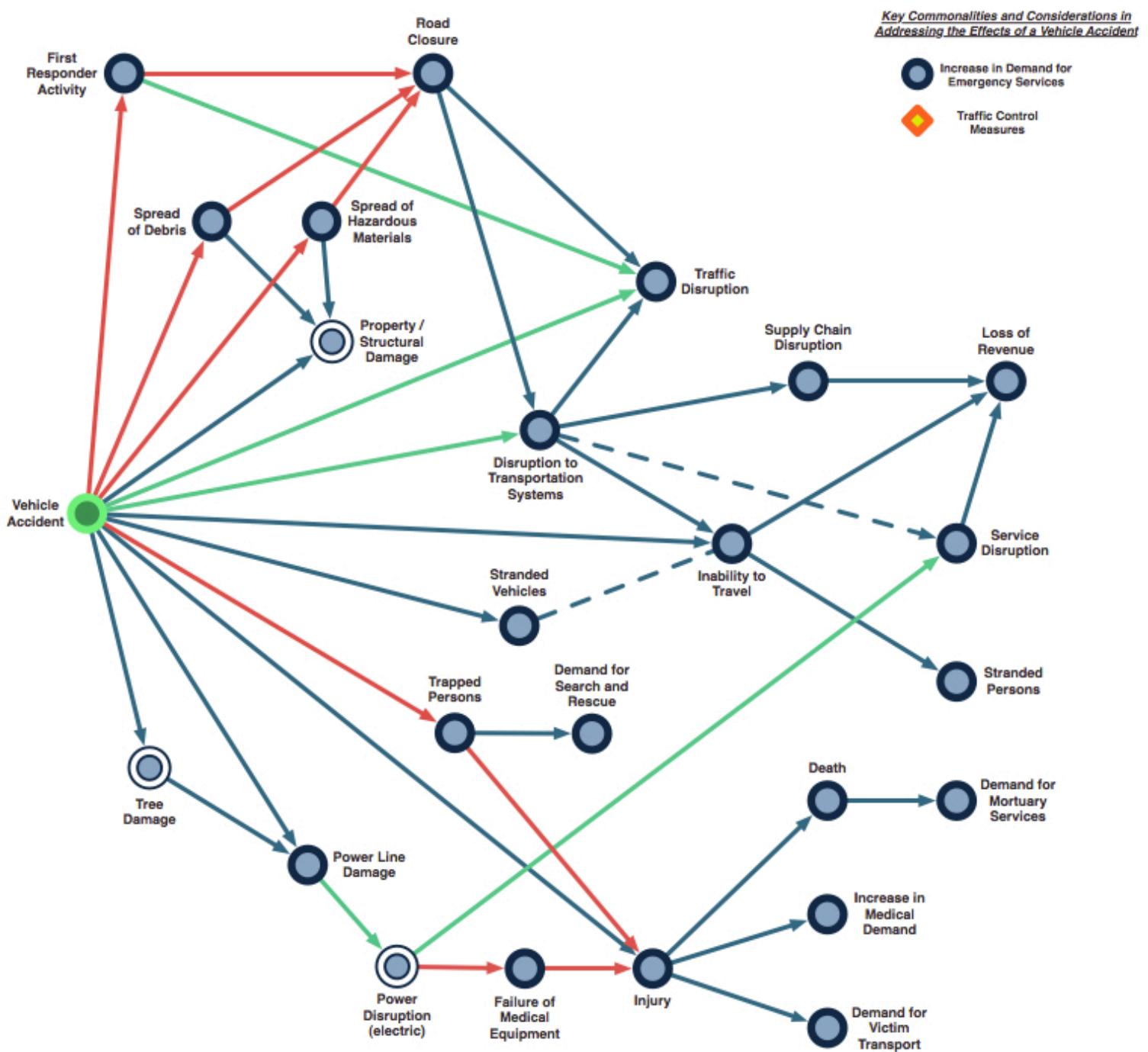
Z.30. TRANSPORTATION SYSTEMS DISRUPTION



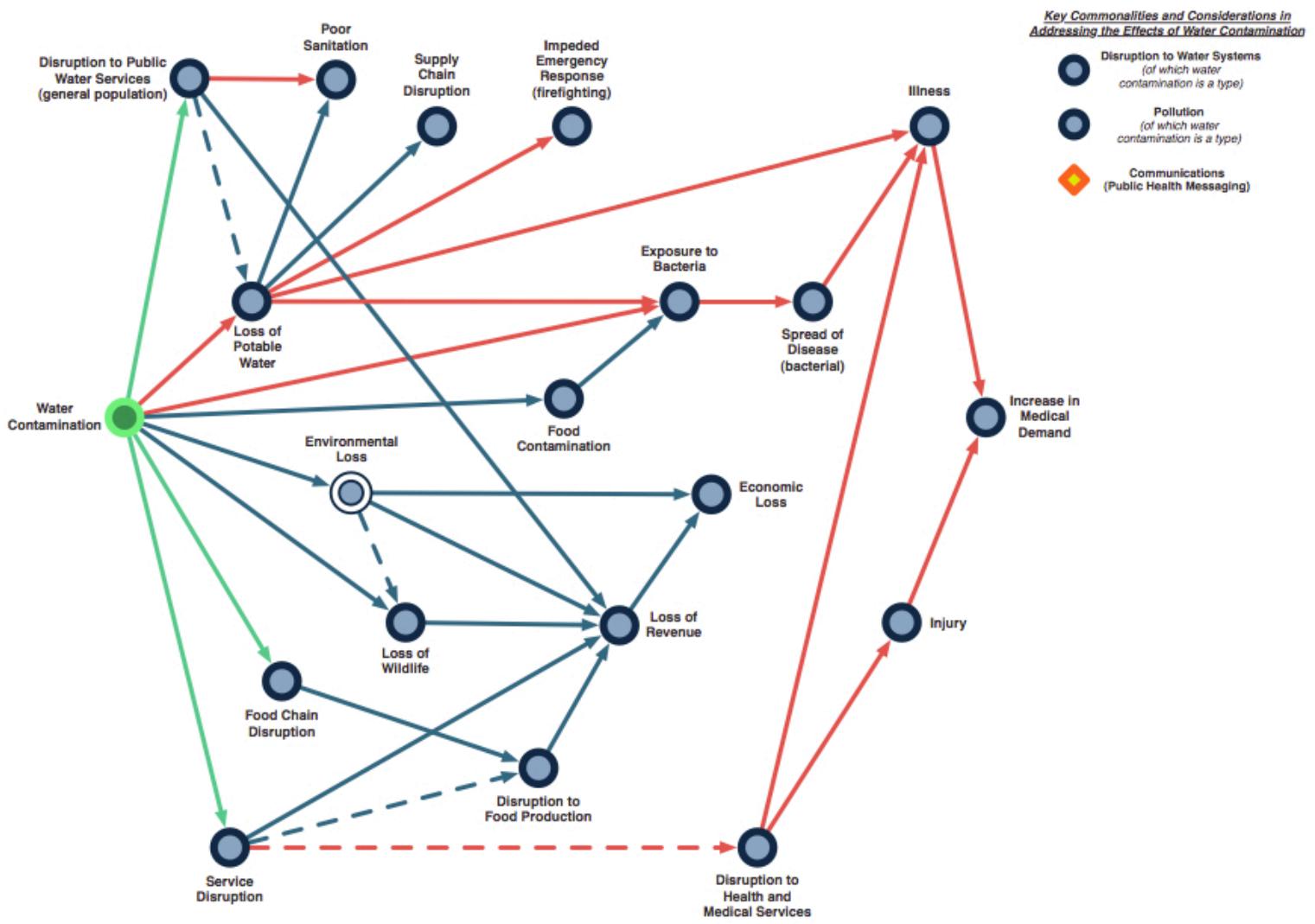
Z.31. TREE DAMAGE



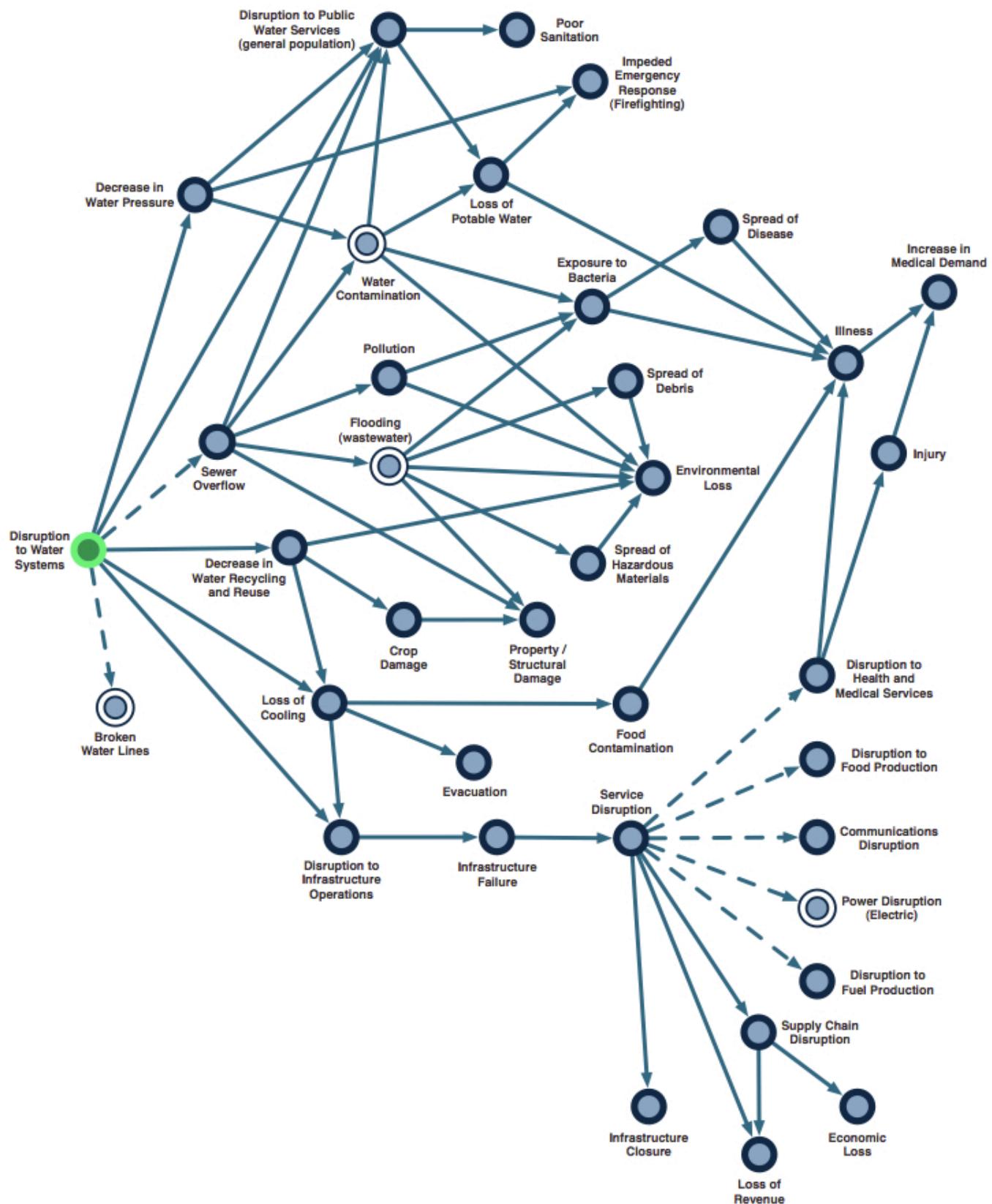
Z.32. VEHICLE ACCIDENT



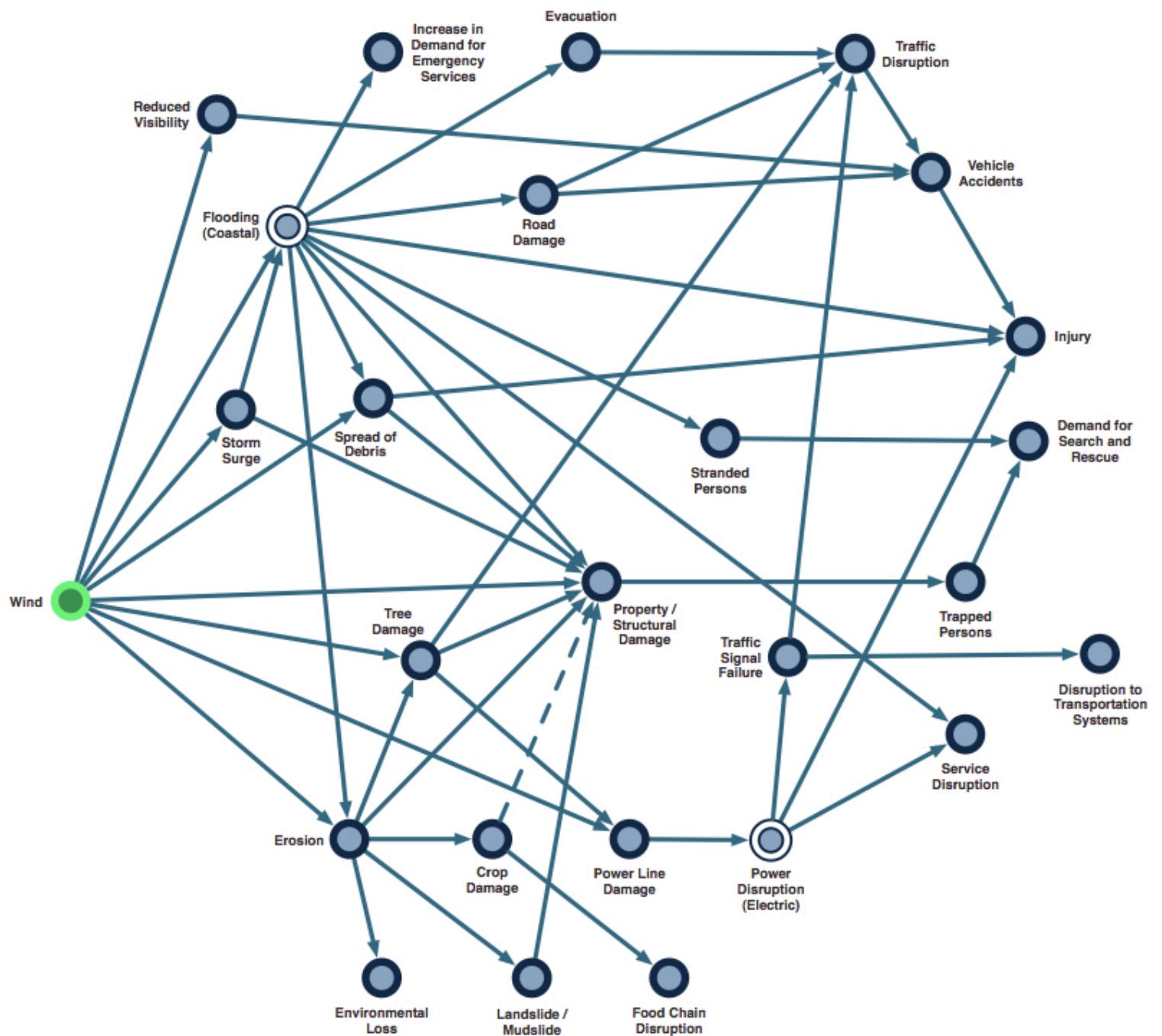
Z.33. WATER CONTAMINATION



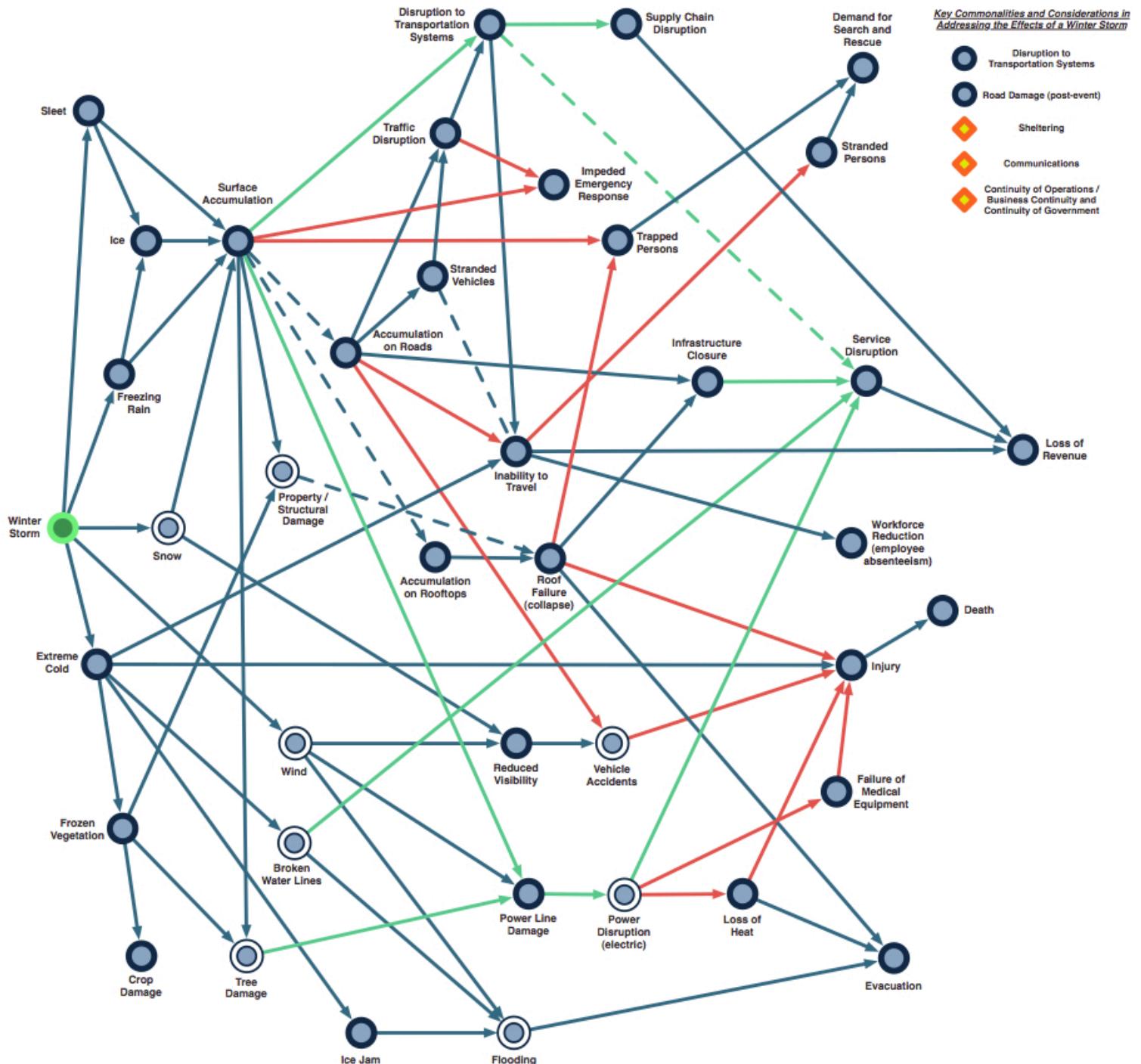
Z.34. WATER SYSTEMS DISRUPTION



Z.35. WIND

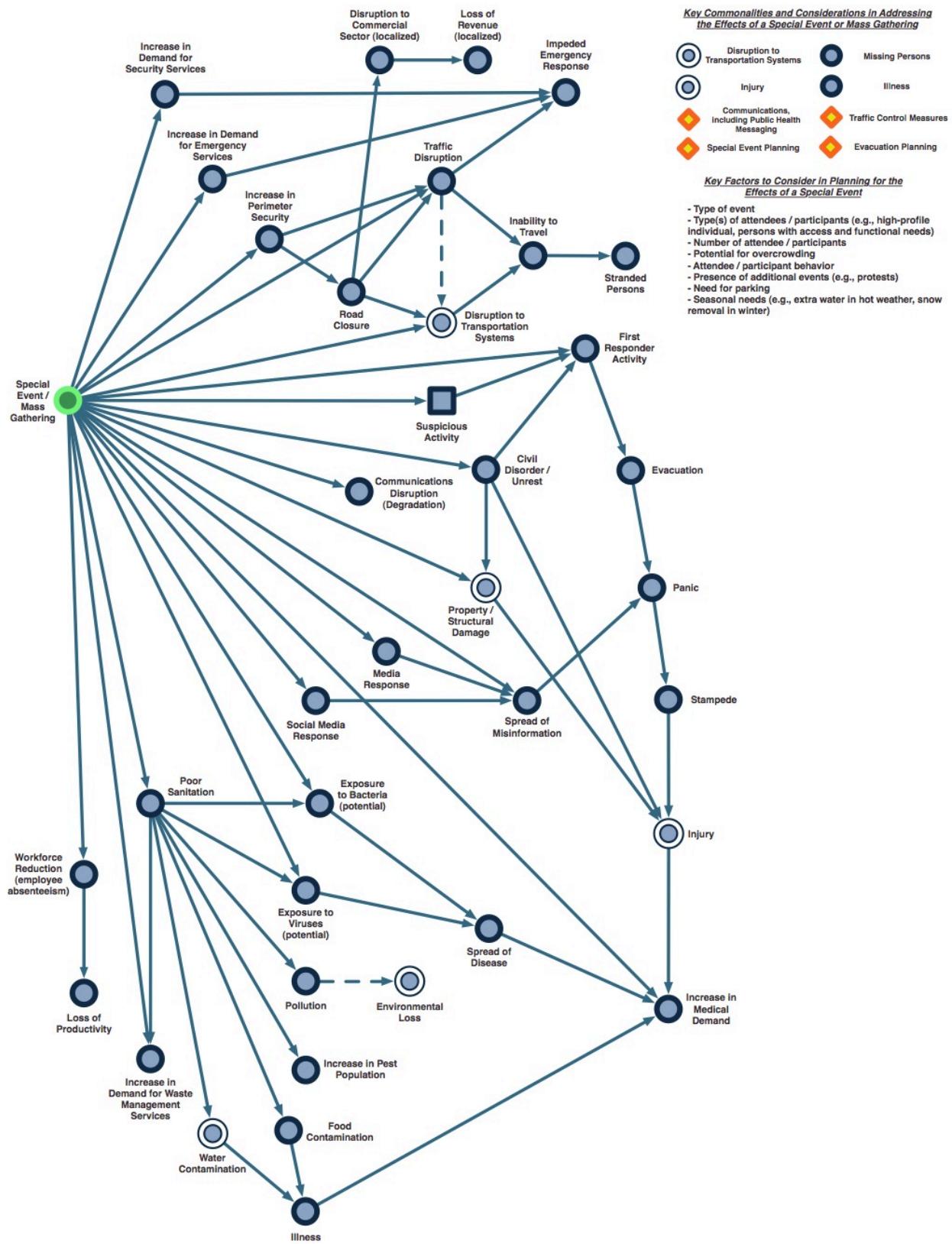


Z.36. WINTER STORM



SPECIAL EVENT NETWORK

Z.37. SPECIAL EVENT / MASS GATHERING



GLOSSARY OF CYBER TERMINOLOGY

Z.38. GLOSSARY OF CYBER TERMINOLOGY

INTELLIGENCE GATHERING (RECONNAISSANCE)

Open-Source Collecting	The act of collecting publicly available information to exploit and disseminate in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.
Phishing	A digital form of social engineering that uses authentic-looking – but bogus – emails to request information from users or direct them to a fake Web site that requests information.
Port Scanning	Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).
Smishing (texts)	Short for SMS Phishing, smishing is a variant of phishing email scams that instead utilizes Short Message Service (SMS) systems to send bogus text messages.
Social Engineering (e.g., phone calls, emails, web redirects)	A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign while actually malicious.
Spear Phishing / Whaling	A type of phishing attack that focuses on a single user or department within an organization, addressed from someone within the company in a position of trust and requesting information such as login credentials (e.g., passwords).
Vulnerability Scanning	The automated process of proactively identifying security vulnerabilities of computing systems in a network to determine if and where a system can be exploited and/or threatened.
Web / Application Scanning	Sending packets or requests to another system to gain information to be used in a subsequent attack.

DELIVERY MECHANISM

Cross-Site Scripting

The injection of malicious code through a vulnerability on a benign website to acquire the permissions of scripts generated by the website; thereby, compromising the confidentiality and integrity of data transfers between the website and clients.

Internet / Web Exploitation (compromised websites)

The use of a particular site – possibly an illegitimate replica of an actual site – that hosts an exploit to be downloaded or malicious web pages, which activate when a vulnerable web browser or browser plug-in visits.

Poison

There are a number of different types of poisoning (e.g., session poisoning, cache poisoning, cookie poisoning) in which each differs in method, but allows the attacker to transmit data and/or force the user or computer to unknowingly access illegitimate and possibly harmful websites, files, etc.

Targeted Attack

An attack that has been aimed at a specific user, company, or organization.

TOOLS AND TECHNIQUES

Botnets

A network of remotely controlled systems (e.g., bots, short for robots) used to coordinate attacks and distribute malware, spam, and phishing scams.

Buffer Overflow

A condition when a program puts more input in a data holding area (i.e., buffer) than capacity allocated, overwriting other information and thereby crashing a system or executing malicious code.

Privilege Escalation by URL Manipulation

The act of altering the parameters of a URL to gain access to more resources or functionality of a website than normally allowed.

Malware

A virus, worm, Trojan horse, or other code-based malicious entity that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

SQL Injection Fault

A form of attack on a database-driven website in which the attacker takes advantage of unsecure code by altering the database search to obtain unauthorized access to sensitive information.

Trojan [e.g., remote access Trojan (RAT)]

A computer program that masquerades as a useful program with hidden and potentially malicious functions to evade security mechanisms, sometimes by exploiting legitimate authorizations of a system.

Virus

A program that “infects” computer files, usually executable programs, by inserting a copy of itself into other files when the files are executed (e.g., opened or run by a user).

Vulnerability Exploitation

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Worm

An independent, self-replicating, self-propagating, and self-contained computer program that uses networking mechanisms to reproduce copies of itself from one system to others across a network – unlike viruses, worms do not require human involvement to propagate.

This page is intentionally blank.

WORKSHEETS

APPENDIX AA. WORKSHEETS

Complimenting a number of methodologies/techniques are worksheets – fillable forms to aid in the completion of an analysis. **CRT worksheets are available in Microsoft Word format upon request.**

APPENDIX AA

ANTICIPATORY FAILURE DETERMINATION	AA-4
Step 1: Formulate the “Original Problem”	AA-4
Step 2: Identify the Success Scenario	AA-4
Step 3: Localize the Failure	AA-4
Step 4: Formulate and Amplify the Invert Problem.....	AA-5
Step 5: Search for Solutions.....	AA-5
Step 6: Formulate Hypotheses and Design Tests to Verify	AA-7
Step 7: Correct the Failure	AA-7
BENEFIT-COST ANALYSIS.....	AA-8
Step 1: Characterize the System.....	AA-8
Step 2: Baseline Risk Assessment	AA-8
Step 3: Identify and Appraise Alternatives	AA-9
Step 4: Compare Alternatives	AA-10
Step 5: Document the Analytic Process and Results	AA-10
DEFINING A SYSTEM	AA-12
Step 1: Establish the Security Context.....	AA-12
Step 2: Articulate the Key Risk Questions.....	AA-12
Step 3: Develop a Conceptual Model	AA-13
Step 4: Identify Available Resources.....	AA-13
Step 5: Select Tools and Techniques	AA-13
DEFINING THE SECURITY CONTEXT.....	AA-14
Step 1: Identify the Proetctor	AA-14
Step 2: Identify the assets	AA-14
Step 3: Identify the threats	AA-14
Step 4: Describe the Situation.....	AA-14
DIVERGENT-CONVERGENT THINKING.....	AA-16
Step 1: Identify Key Risk Question	AA-16
Step 2: Divergent Thinking (Summary of Responses)	AA-16
Step 3: Convergent Thinking (Summary of Groupings).....	AA-17
Step 4: Summary and Additional Results	AA-18
EVENT TREE ANALYSIS.....	AA-20
Step 1: Identify Initiating Event.....	AA-20
Step 2: Determine Greatest Influence	AA-20
Step 3: Decide on the Temporal or Causal Order	AA-20
Step 4: Identify Event Options.....	AA-20
Step 5: Construct Event Tree	AA-21
Step 6: Identify Decisions	AA-21
Step 7: Assess the Implications.....	AA-21

EXPERT OPINION ELICITATION PROCESS	AA-22
Step 1: Need Identification	AA-22
Step 2: Select Study Level and Study Leader	AA-22
Step 3: Identify and Select Peer Reviewers	AA-22
Step 4: Identify and Select Experts	AA-22
Step 5: Identify and Select Observers	AA-23
Step 6: Prepare read-Ahead Materials for Experts and Peer Reviewers	AA-23
Step 7: Identification, Selection, and Development of Technical Issues	AA-23
Step 8: Elicitation of Opinions.....	AA-24
Step 9: Documentation and Communications.....	AA-24
FAILURE MODES AND EFFECTS TEMPLATE	AA-26
HAZARD OPERABILITY ANALYSIS TEMPLATE.....	AA-28
OUTSIDE-IN THINKING	AA-30
Step 1: List All Key Forces.....	AA-30
Step 2: Focus on Key Factors	AA-30
Step 3: Assess the Affect	AA-31
Step 4: Determine Impact	AA-31
PRELIMINARY HAZARD MATRIX TEMPLATE	AA-32
PROBLEM RESTATEMENT AND ISSUE.....	AA-34
Step 1: Articulate the Original Question.....	AA-34
Step 2: Explore Variations of the Original Question	AA-34
Step 3: Settle and Describe the Final Question.....	AA-36
RISK REGISTER TEMPLATE.....	AA-38
SUPPLIER INPUT PROCESS OUTPUT CUSTOMER TEMPLATE	AA-40
SYSTEM DESCRIPTION METHODOLOGY	AA-42
Step 1: Define the Objective(s) of the System.....	AA-42
Step 2: Articulate the Success Scenario(s).....	AA-42
Step 3: Define System Failure	AA-42
Step 4: Utilize the SIPOC Diagram	AA-42

ANTICIPATORY FAILURE DETERMINATION

STEP 1: FORMULATE THE “ORIGINAL PROBLEM”

Create a detailed description of the system being analyzed to include:

- *Naming the system*
- *Stating the system’s purpose*
- *Describing the failure that is being analyzed*

STEP 2: IDENTIFY THE SUCCESS SCENARIO

To further describe the system it is important to model its success scenario or the different phases of operation and the expected outcomes that must be met in each of the phases. A categorical way to dissect the system’s components are according to the following scheme:

- *Most critical*
- *Weak or dangerous functions*
- *Operations in the system*

Operations or Phases	Results

STEP 3: LOCALIZE THE FAILURE

Identify the phase or part of the system in which the actual event (or postulated event) has taken place.

STEP 4: FORMULATE AND AMPLIFY THE INVERT PROBLEM

4.1 INVERT PROBLEM

Original Problem:	<i>How did Event Y occur?</i>
Inverted Problem:	<i>How can I make Event Y occur?</i>

4.2 AMPLIFY OR EXAGGERATE INVERTED PROBLEM

Inverted Problem:	<i>How can I make Event Y occur?</i>
Amplified Inverted Problem:	<i>How can I amplify Event Y occurrence (e.g., widespread, constant)?</i>

STEP 5: SEARCH FOR SOLUTIONS

5.1 SEARCH FOR APPARENT OR OBVIOUS SOLUTIONS

This failure has occurred or was intentionally created in the following areas:

5.2 IDENTIFY RESOURCES

Identify resources required for the occurrence of a given phenomenon/failure event:

Find necessary resources in the system or its surroundings:

5.3 UTILIZATION OF RESOURCES AND SEARCHING FOR NEEDING EFFECTS

Create or identify less obvious resources:

--

5.4 ARIZ (ALGORITHM FOR INVENTING PROBLEM SOLVING) FOR AFD

At this point in time it is important to revisit the questions we have been asking in steps 5.1, 5.2 and 5.3 like:

What physical effect or principle can create the desired failure?	
What resources do I need to implement this principle?	
What resources do I have?	

In some cases the problem that exists may not be solved completely. Yet, there may be ways to solve for the cause of the desired failure in part. In these cases we develop a secondary problem.

Identify the “ideal solution”:	
The Innovation Guide:	
Targeting the technical and physical contradictions:	
Applying the separation principles:	
Substance-Field Analysis:	
The Operator Method:	

STEP 6: FORMULATE HYPOTHESES AND DESIGN TESTS TO VERIFY

Formulate the hypothesis as to how the failure occurred (or could occur):

Specify whatever tests are required to prove this hypothesis (or demonstrate feasibility):

STEP 7: CORRECT THE FAILURE

Identify how the failure can be mitigated:

BENEFIT-COST ANALYSIS

STEP 1: CHARACTERIZE THE SYSTEM

Define the objectives of the system as it relates to the decision maker:

Identify and describe the elements of the system:

Element	Description

Describe how these elements interact to achieve higher-level objectives:

Element	Interaction Description

STEP 2: BASELINE RISK ASSESSMENT

Understand how and why the system can fail to meet objectives due to failure of its basic elements:

Objective	Failure Description

Understand how and why the basic system elements can fail or be made to fail:

Element	Failure Description

Understand the severity of each failure mode or scenario:

Failure	Severity Description / Rating

Understand the likeliness of occurrence for each failure mode or scenario:

Failure	Likelihood Description / Frequency

STEP 3: IDENTIFY AND APPRAISE ALTERNATIVES

Develop a set of alternative countermeasures or mitigation options:

Mitigation Option	Description

Develop a set of evaluation criteria consistent for each option considered:

Mitigation Option	Evaluation Criteria

Appraise each on the basis of the considerations described in the article on benefit-cost analysis:

Failure	Likelihood Description / Frequency

STEP 4: COMPARE ALTERNATIVES

Utilize methodologies such as Weighted Ranking, Sorting, or Devil's Advocacy to:

- Aggregate appraisals of evaluation into benefit and cost scores
- Compare the disaggregated scores
- Rank order alternatives
- Challenge the Results via Alternative Analysis

STEP 5: DOCUMENT THE ANALYTIC PROCESS AND RESULTS

This page is intentionally blank.

DEFINING A SYSTEM

STEP 1: ESTABLISH THE SECURITY CONTEXT

Define the protector:

Identify the protector's assets/values:

Identify threats to the protector:

Describe the relation between the threats and assets/values (matrices may help):

EXAMPLE	Threat 1	Threat 2
Asset 1		
Asset 2		

STEP 2: ARTICULATE THE KEY RISK QUESTIONS

STEP 3: DEVELOP A CONCEPTUAL MODEL

The Suppliers Inputs Process Outputs Customer (SIPOC) diagram may support this step.

STEP 4: IDENTIFY AVAILABLE RESOURCES

Timeframe:	
Number of Analysts:	
Required Skillsets:	
Technology Required (e.g., software):	

STEP 5: SELECT TOOLS AND TECHNIQUES

Utilize the appendices of methodologies and brainstorming techniques for identifying the best tools and technique

DEFINING THE SECURITY CONTEXT

STEP 1: IDENTIFY THE PROECTOR

STEP 2: IDENTIFY THE ASSETS

STEP 3: IDENTIFY THE THREATS

STEP 4: DESCRIBE THE SITUATION

This page is intentionally blank.

DIVERGENT-CONVERGENT THINKING

Date:	Facilitator:
-------	--------------

STEP 1: IDENTIFY KEY RISK QUESTION

Clearly state the key risk question for this brainstorming activity in the box below. There should be only one.

STEP 2: DIVERGENT THINKING (SUMMARY OF RESPONSES)

List all responses from the Divergent Thinking phase of this activity in the box below.

STEP 3: CONVERGENT THINKING (SUMMARY OF GROUPINGS)

Summarize all groupings and associated elements in the boxes below. Use one box per grouping.

Category:
Elements:

Category:
Elements:

Category:
Elements:

Category:
Elements:

Category:
Elements:

Category:
Elements:

Category:
Elements:

STEP 4: SUMMARY AND ADDITIONAL RESULTS

Summarize the analysis, details of any additional results, comments, caveats on the analysis, etc.

This page is intentionally blank.

EVENT TREE ANALYSIS

STEP 1: IDENTIFY INITIATING EVENT

Identify an initiating event that may give rise to unwanted consequences:

STEP 2: DETERMINE GREATEST INFLUENCE

Decide which events, factors, or decisions (i.e., variables) will have the greatest influence on the alternatives or hypotheses identified in Step 1:

Event, Factor, or Decision	Negative Statement

STEP 3: DECIDE ON THE TEMPORAL OR CAUSAL ORDER

Event Statement	Cause	Consequence

STEP 4: IDENTIFY EVENT OPTIONS

Event Statement	Event Options

STEP 5: CONSTRUCT EVENT TREE

Example:

Initiating Threat Event Occurs	Overall Vulnerability as a Mapping from Initiating Threat Event to Degree of Loss				Resulting Degree of Loss
	Contributors to Protection Vulnerability		Contributions to Response Vulnerability		
	Adversary Defeats Security System	Adversary Executes Attack on Target	Target is Damaged	System is Affected by Damage	Consequence are Mitigated
Security System is Effective					None
	Target Not Accessible				None
		Target is Hard			None
			No Loss Potential		None
				No Realized Loss	None
			Low Loss Potential	Low Realized Loss	Low
				No Realized Loss	None
			Medium Loss Potential	Low Realized Loss	Low
				Medium Realized Loss	Medium
				No Realized Loss	None
			High Loss Potential	Low Realized Loss	Low
				Medium Realized Loss	Medium
				High Realized Loss	High
Security System is Ineffective	Target is Accessible	Target is Fragile			

STEP 6: IDENTIFY DECISIONS

Event Option	Decision Point	Decision Indicator

STEP 7: ASSESS THE IMPLICATIONS

Assess the implications or aftereffects of each alternative on the key risk problem.

EXPERT OPINION ELICITATION PROCESS

STEP 1: NEED IDENTIFICATION

Definition of the goal of the study and relevance of issues to this goal:

STEP 2: SELECT STUDY LEVEL AND STUDY LEADER

Study Level:	
Study Leader:	

STEP 3: IDENTIFY AND SELECT PEER REVIEWERS

Types of Individuals:	
Peer Reviewers:	

STEP 4: IDENTIFY AND SELECT EXPERTS

Panel Size:	
Potential Experts:	
Selection Criteria:	
Removal Criteria:	
Selected Experts:	

STEP 5: IDENTIFY AND SELECT OBSERVERS

Knowledge Areas:	
Observers:	

A list of names with biographical statements of the study leader, technical integrator, technical facilitator, experts, observers, and peer reviewers should be developed and documented.

STEP 6: PREPARE READ-AHEAD MATERIALS FOR EXPERTS AND PEER REVIEWERS

Provide the following to Experts and Observers prior to meeting:

- An objective statement of the study;
- A list of experts, observers, integrators, facilitators, study leader, sponsors, and their biographical statements;
- A description of the facility, systems, equipment and components;
- Basic terminology, definitions that should include probability, failure rate, average time between failures, mean (or average) value, median value, and uncertainty;
- Failure consequence types;
- A description of the expert-opinion elicitation process;
- A related example on the expert-opinion elicitation process and its results, if available;
- Aggregation methods of expert opinions such as computations of percentiles;
- A description of the issues in the form of a list of questions with background descriptions. *Each issue should be presented on a separate page with spaces for recording an expert's judgment, any revisions and comments. Clear statements of expectations from the experts in terms of time, effort, responses, communication, and discussion style and format.*

STEP 7: IDENTIFICATION, SELECTION, AND DEVELOPMENT OF TECHNICAL ISSUES

Develop introductory statement with goal of the study and relevance:

Develop instructions with guidance on expectations in answering questions:

Construct questions:

STEP 8: ELICITATION OF OPINIONS

Follow the steps provided in the methodology.

STEP 9: DOCUMENTATION AND COMMUNICATIONS

Final documentation should include:

- Complete descriptions of the steps
- Initial results
- Revised results
- Consensus results
- Aggregated result spreads and reliability measures

This page is intentionally blank.

FAILURE MODES AND EFFECTS TEMPLATE

Key Process Step or Input	Potential Failure Mode	Potential Failure Effects	SEV	Potential Causes	OCC	Current Controls	DET	RPN	Actions Recommended	Resp.	Actions Taken	SEV	OCC	DET
What is the Process Step or Input?	In what ways can the Process Step or Input fail?	What is the impact on the Key Output Variables once it fails (customer or internal requirements)?	How Severe is the effect to the customer?	What causes the Key Input to go wrong?	How often does cause or FM occur?	What are the existing controls and procedures that prevent either the Cause or the Failure Mode?	How well can you detect the Cause or the Failure Mode?	0	What are the actions for reducing the occurrence of the cause, or improving detection?	Who is Responsible for the recommended action?	Note the actions taken. Include dates of completion.			
								0						
								0						
								0						

This page is intentionally blank.

HAZARD OPERABILITY ANALYSIS TEMPLATE

Item	Keyword	Intersection	Deviation	Cause	Consequence	Safeguards	Action

This page is intentionally blank.

OUTSIDE-IN THINKING

Generic Description of the Problem:	
--	--

STEP 1: LIST ALL KEY FORCES

List all the key forces (social, technological, economic, environmental, and political) that could have an impact on the topic, but over which one can exert little influence (e.g., globalization, social stress, the Internet, or the global economy).

<i>Globalization</i>	<i>Social Stress</i>	<i>Internet</i>	<i>Global Economy</i>

STEP 2: FOCUS ON KEY FACTORS

Focus next on key forces over which an actor or policymaker can exert some influence. In the business world this might be the market size, customers, the competition, suppliers or partners; in the government domain it might include the policy actions or the behavior of allies or adversaries.

Force:	

Force:	

Force:	

Force:	

STEP 3: ASSESS THE AFFECT

Assess how each of these forces could affect the analytic problem.

Force	Affect

STEP 4: DETERMINE IMPACT

Determine whether these forces actually do have an impact on the particular issue based on the available evidence.

Force	Impact

PRELIMINARY HAZARD MATRIX TEMPLATE

Note: Do not be limited by the size or depth of this template. It should be expanded if needed to meet the specific needs of your system. There are no limitations on the breadth or depth of the Hazard Matrix.

Hazard Group	Potential Areas of Failure					
	Structural	Electrical	Pressure	Leakage/Spillage	Mechanical	Procedural
Collision/Mechanical Damage						
Loss of Habitable Atmosphere						
Corrosion						
Contamination						
Electric Shock						
Fire						
Pathological						
Psychological						
Temperature Extremes						
Radiation						
Explosion						

This page is intentionally blank.

PROBLEM RESTATEMENT AND ISSUE DEVELOPMENT

STEP 1: ARTICULATE THE ORIGINAL QUESTION

Write down the original key risk question.

STEP 2: EXPLORE VARIATIONS OF THE ORIGINAL QUESTION

Provided below are six strategies designed to help analysts and decision makers properly identify the most significant problem statement or issue. The following processes may be used in any order and should be used together to identify the central issues and alternative ways of stating them.

2.1 PARAPHRASE THE ORIGINAL QUESTION

Redefine the issue without losing the original meaning.

2.2 FLIP THE ORIGINAL QUESTION 180-DEGREES

Turn the issue on its head. Is the issue the one asked or the opposite of it?

2.3 BROADEN THE FOCUS OF THE ORIGINAL QUESTION

Instead of focusing on only one piece of the puzzle, step back and look at several pieces together. What is the issue before you connected to?

2.4 NARROW THE FOCUS OF THE ORIGINAL QUESTION

Can the issue be broken down further? Take the question and ask about the components that make up the problem.

2.5 REDIRECT THE FOCUS OF THE ORIGINAL QUESTION

What outside forces impinge on this issue? Is deception involved?

2.6 ASK “WHY” OF THE ORIGINAL QUESTION

Ask “why” of the initial issue or question. Develop a new question based on the answer. Then ask “why” of the second question and develop new question based on that answer. Repeat this process until you believe the real problem emerges.

STEP 3: SETTLE AND DESCRIBE THE FINAL QUESTION

Finalize the question. This question should be as significant as possible.

Provide a short summary of the nuances underlying this revised question.

This page is intentionally blank.

RISK REGISTER TEMPLATE

Function	Risk Event	Risk Cause	Impact / Consequence	Existing Mitigations	Adequacy of Existing Mitigations	Action	Additional Mitigations	Deliverables	Required Resources	Owner	Estimated Timeframe	Dependencies / Interdependencies
Maintain public confidence	<i>Internal information implicating serious processing issues is released to the public</i>	<i>Insider threat</i>	<i>Loss of confidence Loss of stakeholders/ customers Loss of reputation</i>	<i>IA training and programs</i>	<i>Inadequate</i>	<i>Treat</i>	<i>Fix the processing issues</i>	<i>Process and IT work</i>	<i>Consultants</i>	<i>Division</i>	<i>1 - 2 years</i>	<i>Systems, Applications, vendors</i>

This page is intentionally blank.

SUPPLIER INPUT PROCESS OUTPUT CUSTOMER TEMPLATE

<i>Who are the interdependencies providing support or inputs to the function?</i>		<i>What do the interdependencies provide to the process?</i>		<i>What are the start and end points of the process and the major steps in the process?</i>		<i>What product or service does the process deliver to the customer?</i>		<i>Who are the customers for the product or service? What are their requirements?</i>	
SUPPLIERS		INPUTS		PROCESS		OUTPUTS		CUSTOMERS	
1		1		Start Point:		1		1	
		2				2			
		3				3			
		4				4		2	
		5		Operation or Activity		5		3	
		6		1		6			
		7		2		7			
2		1		3		8			
		2		4		9			
		3		5		10		4	
3		1		6		11			
		2		7		12			
		3		8		13			
		4		9		14		5	
4		1		10		15		6	
		2		11		16		7	
		3		End Point:		17			
		4				18		9	
		5				19			
		6				20			

This page is intentionally blank.

SYSTEM DESCRIPTION METHODOLOGY

STEP 1: DEFINE THE OBJECTIVE(S) OF THE SYSTEM

STEP 2: ARTICULATE THE SUCCESS SCENARIO(S)

Success Scenario	Capability	Duration	Environment

STEP 3: DEFINE SYSTEM FAILURE

Failure	Gradation (minor, major, catastrophic)

STEP 4: UTILIZE THE SIPOC DIAGRAM

Utilize the SIPOC Diagram to define all outputs, inputs, and state variables for methodology steps 4 - 7.

This page is intentionally blank.

| SUPPORTING APPENDICES

This page is intentionally blank.

APPENDIX BB. GLOSSARY

Terminology	Definition
All-Hazards	A grouping classification encompassing all conditions, environmental or manmade, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or alternatively causing functional degradation to social, economic, or environmental aspects.
Anchoring	A psychological heuristic when estimates are made and adjusted based on the initial known information.
Anticipator Failure Determination (AFD)	A problem solving tool that is used to reveal potential failure modes in a system.
Asset	A person, structure, facility, information, material, or process that has value.
Assumption	A statement accepted or supposed as true without proof or demonstration; an unstated premise or belief.
Benefit-Cost Analysis (BCA)	The evaluation of the overall cost-effectiveness of one or more mitigation options – considering the range of potential benefits, costs and other factors.
Business Continuity	The ability of an organization to continue to function before, during, and after a disaster.
Business Impact Analysis (BIA)	A method of identifying the consequences of failing to perform a function or requirement.
Business Process Analysis (BPA)	A method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, data, interdependencies, and alternate locations inherent in the execution of a function or requirement.
Cause and Effect Diagram	A visual representation of possible contributing factors to an outcome of concern; also known as a fishbone diagram or an Ishikawa Diagram.
Consequence	An effect of an event, incident, or occurrence.
Continuity	The ability to provide uninterrupted services and support, while maintaining organizational viability, before, during, and after an event that disrupts normal operations.

Terminology	Definition
Continuity of Government (COG)	A coordinated effort within the executive, legislative, or judicial branches of the Federal Government to ensure that National Essential Functions continue to be performed during a catastrophic emergency.
Continuity of Operations (COOP)	An effort within the Executive Office of the President and individual departments and agencies to ensure that essential functions continue to be performed during disruption of normal operations.
Countermeasure	An action, measure, or device intended to reduce an identified risk.
Data Classification System	A system/process for classifying information into categories based on the extent to which it must be protected.
Decision Variable	An input variable that is controllable by the decision maker.
Defining a System	A concept that builds upon the security context by identifying what systematically decomposing a system into assets will directly bear on the interests of the protector.
Defining the Security Context	Specifies the bounds on what is considered and what is not considered in a risk study.
Delphi Method	A forecasting method that relies on obtaining a consensus from a collection of experts.
Developing Factor-Based Models	Factor-based models are a major part of qualitative risk analysis, where the factors provide the means for breaking down complex problems into more manageable pieces.
Devil's Advocacy	The involvement of challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation.
Divergent-Convergent Thinking	A form of structured brainstorming that generates new analytic ideas, hypotheses and concepts or helps discover previously unimagined hazards, vulnerabilities, and risky situations through an unconstrained creative group process.
Diversity	Distributed or expanded among various types or forms. For example, communications system route diversity is communications routing between two points over more than one geographic or physical path with no common points.
Environmental Variable	An input variable from the environment.
Event Mapping	Organizes the who, what, where, when, why, and how of an event is the goal of this graphic organizer.

Terminology	Definition
Event Tree Analysis	A visual depiction of the downstream events resulting from the occurrence of an initiating event affecting a system.
Exogenous Variable	An input variable from outside a system's boundary.
Expert-Opinion Elicitation Process (EOEP)	A formal, heuristic process of obtaining information or answers to specific questions about certain quantities, called issues, such as failure rates, probabilities of events, failure consequences and expected service lives.
Factor-Based Models	A set of factors (such as values and variables) that describe the past, present, or future state of a complex problem.
Failure Modes and Effects Analysis (FMEA)	A formal systematic approach to identifying how a system could fail, the causes of such failure, and the effects of its occurrence on the system operation.
Fault Tree Analysis (FTA)	A top-down approach for identifying how an undesirable event can happen or be made to happen. A Fault Tree systematically breaks down a single undesirable event in terms of its potential underlying causes.
Federal Continuity Directive (FCD)	A document developed and promulgated by DHS/FEMA, in coordination with the Continuity Advisory Group and in consultation with the Continuity Policy Coordination Committee, which directs Executive Branch organizations to carry out identified continuity planning requirements and assessment criteria.
F-Type	Models that describe predictor variables or state variables (the factors) that relate to some sort of response variable (the output).
Hazard	A natural or man-made source or cause of harm or difficulty.
Hazard and Operability Analysis (HazOp)	A bottom-up approach that identifies potential hazards and operability complications within a system.
Heuristic	Involving or serving as an aid to learning, discovery, or problem-solving by experimental and especially trial-and-error methods
Hierarchical Holographic Modeling (HHM)	A technique for examining an issue from multiple points of view to identify the various sources of risk present in a large-scale system.
Hypothesis	An idea or theory that is not proven but that leads to further study or discussion.
Impact	See <i>Consequence</i>

Terminology	Definition
Incident	Occurrence, caused by either human action or natural phenomena, that may cause harm and that may require action.
Influence Diagrams	A compact visual representation of a decision situation that shows how a set of variables interact with one another (also known as a relevance diagram, decision diagram, or a decision network).
Input Variables	Input variables are what go into a system. There are three types: decision variables, environmental variables, and exogenous variables.
Interdependency	Mutually reliant relationship between entities (objects, individuals, or groups). The degree of interdependency does not need to be equal in both directions.
Interval	Interval scales build upon ordinal scale variables by assigning numbers to objects such that the differences between the numbers can be meaningfully interpreted (e.g., temperatures).
Key Risk Question	A key risk question is generally described as a question that focuses risk analysis in consideration of analysis purpose and scope. For example, it may be “how can we prevent the spread of a pandemic illness in our organization?”
Likelihood	The chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities.
Measurement of Intangibles	The ability to assign quantitative measurement to characteristics that are generally believed to be immeasurable.
Mitigation	An ongoing and sustained action to reduce the probability of, or lessen the impact of, an adverse incident.
Model	An approximation, representation, or idealization of selected aspects of the structure, behavior, operation, or other characteristics of a real-world process, concept, or system.
National Continuity Policy	It is the policy of the United States to maintain a comprehensive and effective continuity capability, composed of Continuity of Operations and Continuity of Government programs, in order to ensure the preservation of our form of government under the Constitution and the continuing performance of National Essential Functions under all conditions (Presidential Policy Directive-40, <i>National Continuity Policy</i>).

Terminology	Definition
Nominal	Nominal scales assign numbers as labels to identify objects or classes of objects. Order has no meaning and the difference between identifiers is meaningless.
Ordinal	Ordinal scales build upon nominal scales by assigning numbers to objects to reflect a rank ordering on an attribute in question. The difference between ordinal variables is not consistent across the scale.
Outputs Variable	A variable that defines what comes out of a system; an output variable can be used to determine how well the system is performing and measure whether a system is meeting its objectives.
Outside-In Thinking	Used to identify the full range of basic forces, factors, and trends that would indirectly shape an issue.
Pairwise Ranking	A structured analytic technique for ranking a small list of items in priority order, whether by importance, preference or other measure of value.
Preliminary Hazard Analysis (PHA)	A semi-quantitative analysis that is implemented in the earliest stages of system design.
Premortem Analysis	Allows a group of analysts or stakeholders (i.e., team) to examine the various factors that could inhibit the success of a plan.
Probability	A numerical value between zero and one assigned to a random event (which is a subset of the sample space) in such a way that the assigned number obeys three axioms: 1) the probability of the random event $-A\ $ must be equal to, or lie between, zero and one; 2) the probability that the outcome is within the sample space must equal one; and 3) the probability that the random event $-A\ $ or $-B\ $ occurs must equal the probability of the random event $-A\ $ plus the probability of the random event $-B\ $ for any two mutually exclusive events.
Problem Restatement and Issue Development	A technique used to ensure that the central issues and alternative explanations of an issue or problem are identified within the scope and focus of the problem statement.
Process Map	A process map is a graphical depiction of a process, set in a way that allows the workings to be shown.
Protector	Defines the individual at the center of a risk analysis, defines what should be considered as a decision variable vice an input variable, defines the scope of risk considerations (e.g., which people, whose money, what else), etc.

Terminology	Definition
Ratio	Ratio scales have all the attributes of interval scale variables and one additional attribute: ratio scales include an absolute “zero” point.
Redundancy	The state of having duplicate capabilities, such as systems, equipment, or resources. In other words, additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.
Reliability Block Diagram (RBD)	A graphical illustration of how the failures of system’s components interact to cause failure of the entire system.
Resilience	The ability to prepare for and adapt to changing conditions and recover rapidly from operational disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
Return on Investment (ROI)	The calculation of the value of risk reduction measures in the context of the cost of developing and implementing those measures.
Reverse Brainstorming	A structured brainstorming technique that asks how and why a hazard might not occur, and uses the converse of these reasons to suggest how it might actually occur.
Risk	The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequence. With respect to continuity, risk may degrade or hinder the performance of essential functions and affect critical assets associated with continuity operations.
Risk Acceptance	An explicit or implicit decision not to take an action that would affect all or part of a particular risk.
Risk Analysis	A systematic examination of the components and characteristics of risk.
Risk Assessment	A product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.
Risk Avoidance	Strategies or measures taken that effectively remove exposure to a risk.
Risk Control	A deliberate action taken to reduce the potential for harm or maintain it at an acceptable level.

Terminology	Definition
Risk Management	The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken.
Risk Perception	The subjective judgment about the characteristics and/or severity of risk.
Risk Tolerance	The degree to which an entity, asset, system, network, or geographic area is willing to accept risk.
Risk Transfer	The action taken to manage risk that shifts some or all of the risk to another entity, asset, system, network, or geographic area.
Root Cause Analysis	A systematic approach that seeks to identify the origin of a problem.
Round-Robin Brainstorming	Relies on ideas being generated in the absence of discussion for completely free-form thoughts unhindered by group trends or consensus.
Scenario	The hypothetical situation comprised of a threat or hazard, an entity impacted by that threat/hazard, and associated conditions including consequences when appropriate.
Scoping a Risk Study	A process of defining the scope and boundaries of a project utilizing multiple methodologies.
Sorting	A basic structured analytic technique for grouping information to develop insight, identify patterns, uncover trends and spot anomalies.
State Variable	Internal variables that describe what is going on in a system.
Subject-Matter Expert (SME)	An individual with in-depth knowledge in a specific area or field.
Success Scenario	A concise statement of how an organization must perform under all conditions by defining the boundary between failure and success.
System	Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.
System Description Methodology	Provides an approach for completely describing a system of interest.
Systematic	The act of using a careful system or method.
Tangible Data	Factual information (such as measurements or statistics) capable of being precisely identified and discussed or calculated at an actual or approximate value.

Terminology	Definition
Testimonial Data	Proof or evidence provided as factual information.
Threat	A natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
Uncertainty	The degree to which a calculated, estimated, or observed value may deviate from the true value.
V-Type	Models that describe low-level value dimensions (the factors) that relate in some way to higher-level values (the output).
Vulnerability	A physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard.
Vulnerability Assessment	The product or process of identifying physical features or operational attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to hazards.
Weighted Ranking	A technique for ranking and prioritizing different events, vulnerabilities, hazards, threats, countermeasures or other objects with respect to two or more value criteria.
Work Breakdown Structure (WBS)	A dynamic process for defining the products of a project and their relationships.

This page is intentionally blank.

APPENDIX CC. REFERENCES

A Tradecraft Primer: Basic Structured Analytic Techniques. Defense Intelligence Agency. March 2008, pp. 6-67.

A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis. Central Intelligence Agency. Vol. 2, No. 2. June 2005.

Ayyub, Bilal M. *Elicitation of Expert Opinions for Uncertainty and Risks.* Boca Raton: CRC, 2001. Print.

De Feo, Joseph A., and Zion Bar-El. "Creating Strategic Change More Efficiently with a New Design for Six Sigma Process". *Journal of Change Management.* August 2002, pp. 60-80.
<http://www.idealizationtriz.com/pdf_Creating_strategic_change.pdf>.

DHS Risk Lexicon. U.S. Department of Homeland Security, 2010.

Eccles R., Newquist S., and Schatz R. (2007). "Reputation and its Risks." *Harvard Business Review.* February 2007. <<https://hbr.org/2007/02/reputation-and-its-risks>>.

Federal Continuity Directive 1. U.S. Department of Homeland Security, Federal Emergency Management Agency, 2017.

Federal Continuity Directive 2. U.S. Department of Homeland Security, 2013. (Pending revision in 2017)

Fowles, Dr. Jib, and Robert B. Fowles. *Handbook of Futures Research.* Westport: Greenwood, 1978. Print.

Guide for Conducting Risk Assessments. National Institute of Standards and Technology. NIST Special Publication 800-30, Revision 1. September 2012. <http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf>.

Haimes, Yacov Y. *Protection of Critical Complex Transportation Infrastructures.* Transportation Research Board Committee A. 19 March 2001.
<<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.5123&rep=rep1&type=pdf>>.

Haimes, Yacov Y. *Risk Modeling, Assessment, and Management.* Hoboken: John Wiley & Sons, 2009. Print.

Hubbard, Douglas W. *How to Measure Anything: Finding the Value of "intangibles" in Business.* Hoboken: John Wiley & Sons, 2007. Print.

Jones, Morgan D. *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving.* New York: Three Rivers, 1998. Print.

Kaplan, S. and Garrick, B. J. "On the Quantitative Definition of Risk." *Risk Analysis.* Vol. 1, No. 1 1981, pp. 11-27.

Kaplan, Stan, Boris Zlotin, Alla Zusman, and Svetlana Visnepolschi. *New Tools for Failure and Risk Analysis: New Tools for Failure and Risk Analysis: Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring*. Southfield: Ideation International, 1999. Print.

Kaplan, Stan, Yacob Y. Haimes, and B. John Garrick. "Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk." *Risk Analysis*. Vol. 21, No. 5. 2001, pp. 807-820. <<http://onlinelibrary.wiley.com/doi/10.1111/0272-4332.215153/pdf>>.

Klein, Gary A. *The Power of Intuition: How to Use Your Gut Feelings to Make Better Decisions at Work*. New York: Currency/Doubleday, 2003. Print.

Klir, George J. *Facets of Systems Science*. New York: Kluwer, 2001. Print.

Managing Information Security Risk: Organization, Mission, and Information System View. National Institute of Standards and Technology. NIST Special Publication 800-39. March 2011. <<http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>>.

Manunta, Giovanni. *Defining Security*. Diogenes Paper. No. 1. Royal Military College of Sciences: Cranfield Security Centre, March 2000. <<http://www.srsi.org/diogenes.htm>>.

National Infrastructure Protection Plan. U.S. Department of Homeland Security, 2013.

NIPP Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach. U.S. Department of Homeland Security. 2013. <<https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf>>.

Paul, R. Critical Thinking: How to Prepare Students for a Rapidly Changing World. Dillon Beach: Foundation For Critical Thinking, Appendix B. 1995, pp. 521-552.

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard. U.S. Department of Homeland Security. August 2013. https://www.dhs.gov/sites/default/files/publications/ISC_Risk-Management-Process_Aug_2013.pdf.

Strauss, Sheryl. *Security Problems in a Modern Society*. Boston: Butterworth, 1980. Print.

Tversky, Amos, and Daniel Kahneman. "Judgment under Uncertainty: Heuristics and Biases." *Science*. Vol. 185, No. 4157. 27 September 1974, pp. 1124-1131. <<http://people.hss.caltech.edu/~camerer/Ec101/JudgementUncertainty.pdf>>

Vincoli, Jeffrey W. *Basic Guide to System Safety*. New York: Van Nostrand Reinhold, 1993. Print.
