Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

Advanced Risk Analysis for High-Performing Organizations

Christopher Alberts
Audrey Dorofee

Sponsored by the U.S. Department of Defense
© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Changing Operational Environment

From	To
Centralized management control of processes	Distributed management control of processes
Dedicated, stand-alone technologies	Interoperable, networked technologies
Permanent enterprise, defined by organizational chart	Virtual enterprise, defined by mission
One team, one mission	Many teams, one mission
Compartmentalized view of risk (e.g., project, security)	Integrated view of risk

© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Changing Risk Profiles

Changes in operational environments are driving the need for advanced risk analysis techniques.

- The operational environment is becoming more complex (e.g., distributed processes).

- New types of risks have emerged from this complexity.
  - inherited risk
  - new sources of risk (e.g., cyber-security risks)
  - risk from combinatorial effects
  - risk from cascading consequences
  - risk from emergent threats

© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

The Need for Advanced Techniques

High-performing organizations are able to manage traditional risks.

Risks arising from operational complexity are often subtle in nature, but bring the potential for catastrophic consequences.

High-performing organizations have the basic skills needed to manage these new types of risk, but sufficient techniques are not readily available.

© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Key Requirements

High performers need advanced risk management techniques that enable them to

- assume an integrated view of risk (one view that includes process, technology, security, and interoperability risks)
- address the interrelated nature of risk (combinatorial effects and cascading consequences)
- understand the amount of risk that is inherited from partners and collaborators
- characterize the risk arising from the emergent properties of a distributed process

© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

What Is Risk?

The possibility of suffering harm or loss

Risk requires the following conditions:

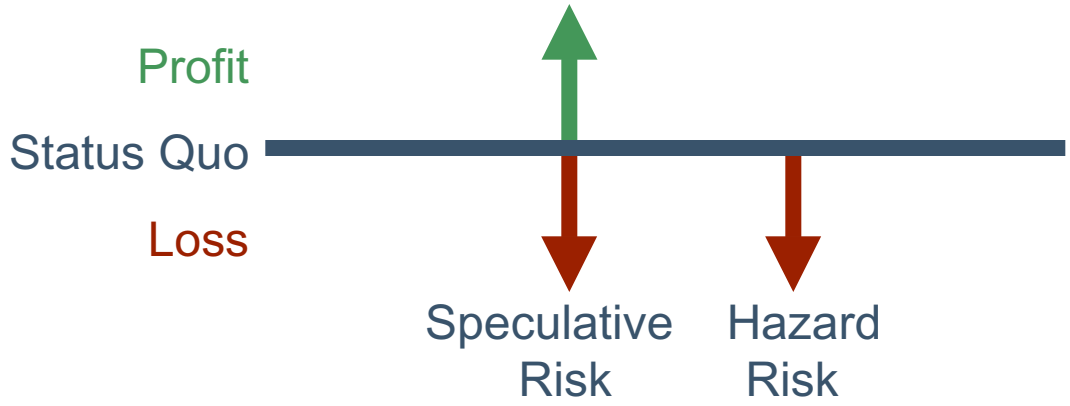
- loss
- uncertainty
- choice

© 2006 by Carnegie Mellon University

Nature of Risk

Speculative (dynamic) – a risk that has profit and loss associated with it

Hazard (static) – a risk that only has loss associated with it



© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Operational Risk[1]

The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events

1. Bank for International Settlements (BIS). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. BIS, 2004. http://www.bis.org/publ/bcbs107.pdf.

© 2006 by Carnegie Mellon University

Sources of Risk During Operations

A broad range of threats must be considered when analyzing the potential for mission success.

© 2006 by Carnegie Mellon University

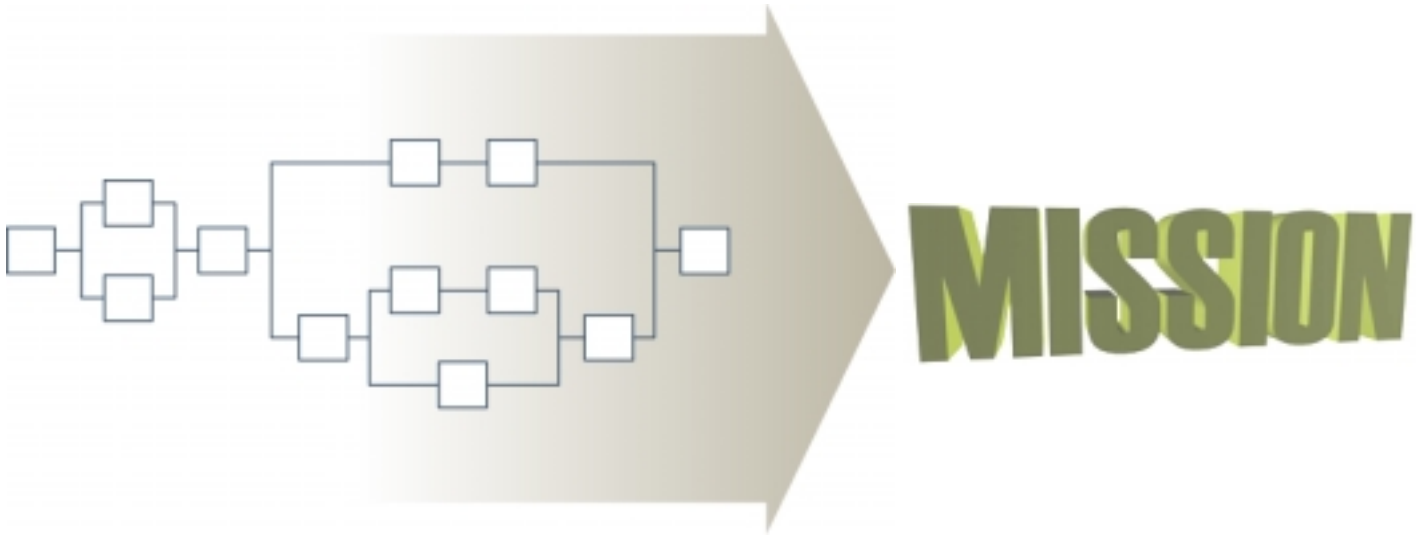
Carnegie Mellon
Software Engineering Institute

Mission

A mission threat is a fundamental flaw, or weaknesses, in the purpose and scope of a work process.

© 2006 by Carnegie Mellon University

Process Design



A design threat is an inherent weakness in the layout of a work process.

© 2006 by Carnegie Mellon University

Activity Management

An activity threat is a flaw, or weaknesses, arising from the manner in which activities are managed and performed.

© 2006 by Carnegie Mellon University

Operational Environment

Operational Environment

An environment threat is an inherent constraint, weakness, or flaw in the overarching operational environment in which a process is conducted.

© 2006 by Carnegie Mellon University

Event Management

An event threat is a set of circumstances triggered by an unpredictable occurrence that introduces unexpected change into a process.

© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Mission Risk

The possibility that a mission might not be successfully achieved

© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Mission Assurance

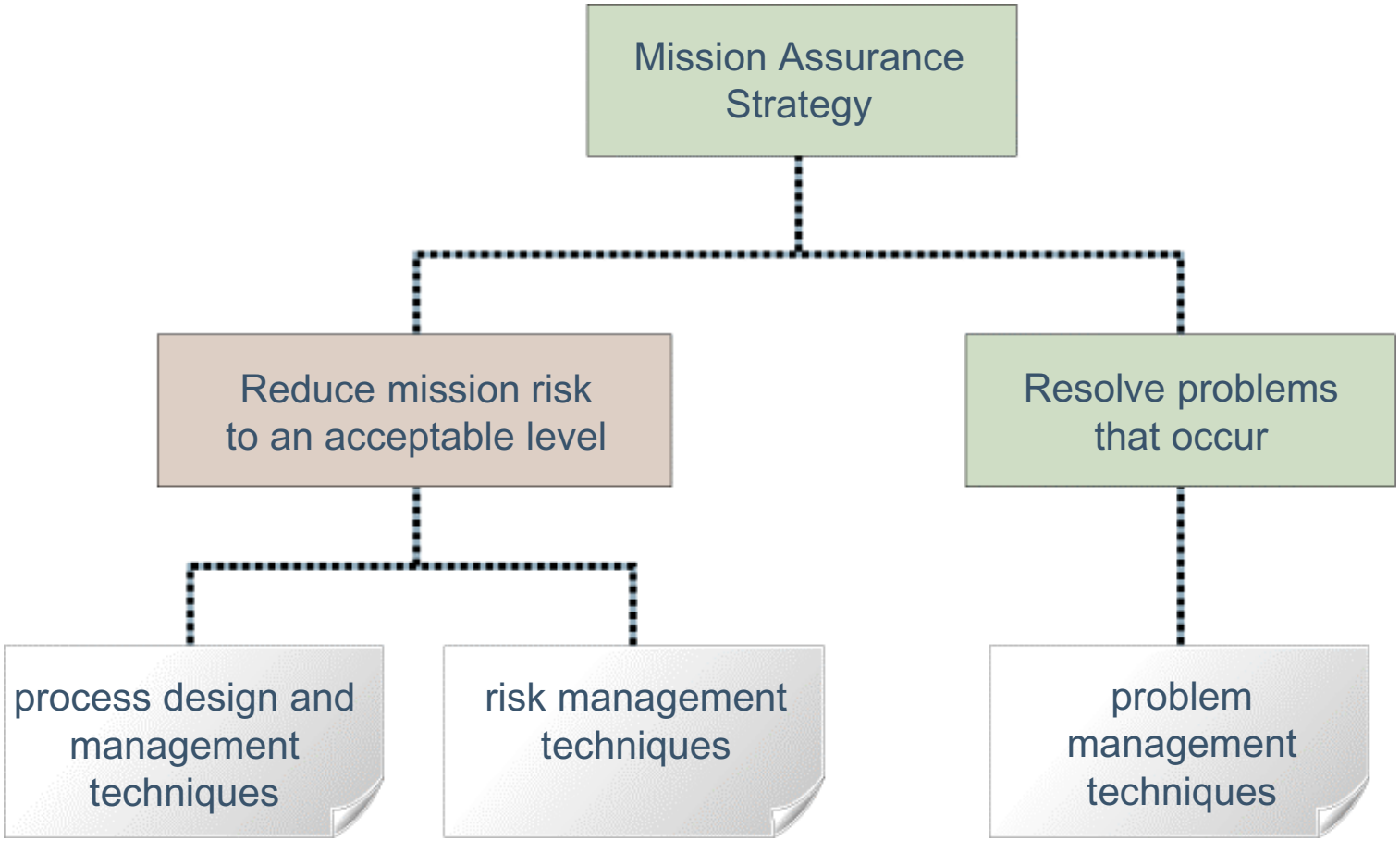
Establishing a reasonable degree of confidence in mission success

Mission assurance is achieved by ensuring that risk to the mission (i.e., mission risk) is within tolerance.

A key aspect of mission assurance is its dual focus on outcome and execution.

© 2006 by Carnegie Mellon University

Mission Assurance Strategy



© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

What is MAAP?

MAAP is a protocol, or heuristic, for determining the mission assurance of an operational process or system.

© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Key Characteristics of MAAP

Applies an engineering approach to risk analysis

Designed for highly complex environments (multi-organization, system of systems)

Provides an in-depth analysis of processes, relationships, and dependencies

Characterizes the risk of mission failures

- process performance risk
- security risk
- operational environment risk

© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Structured Analysis of Performance

MAAP analyzes process performance in multiple operational states

- normal, or expected, operational conditions
- unusual circumstances, or occurrences, triggered by external events

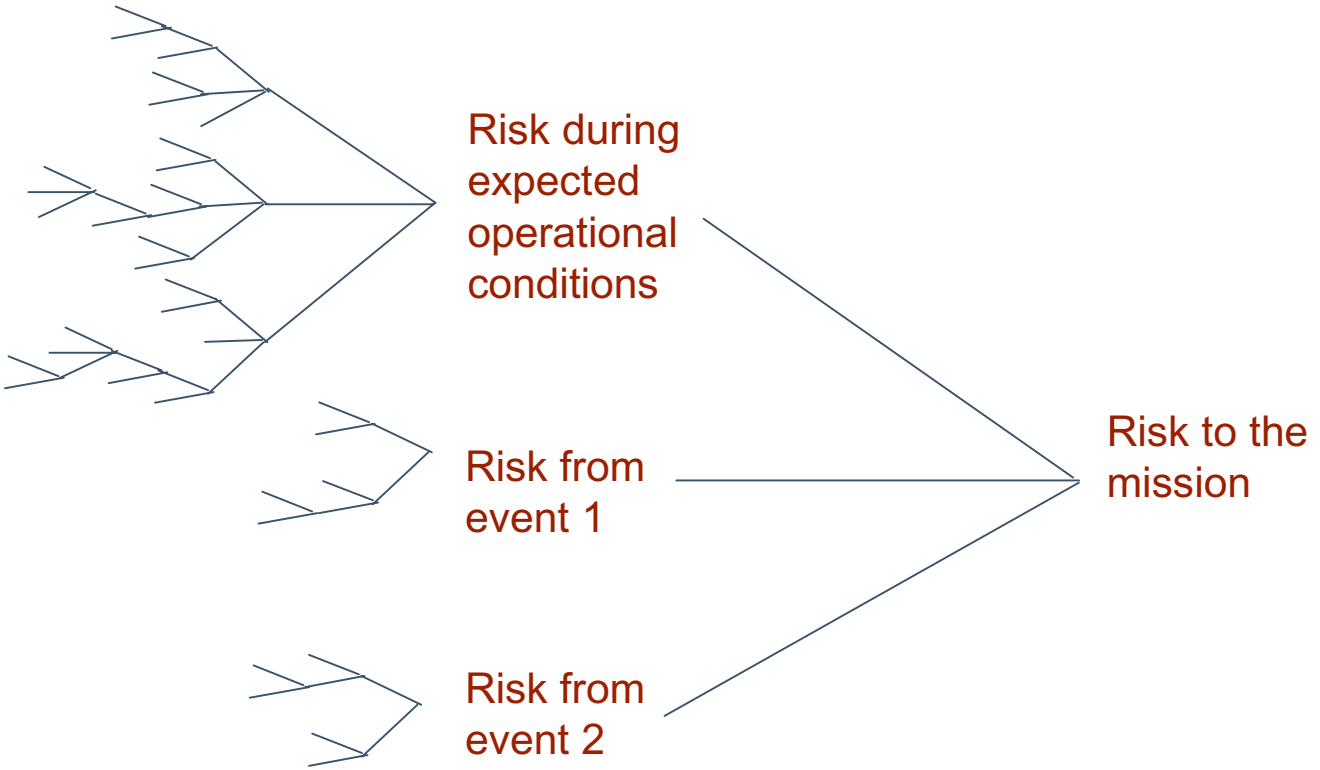
© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Analyzing Multiple States

© 2006 by Carnegie Mellon University

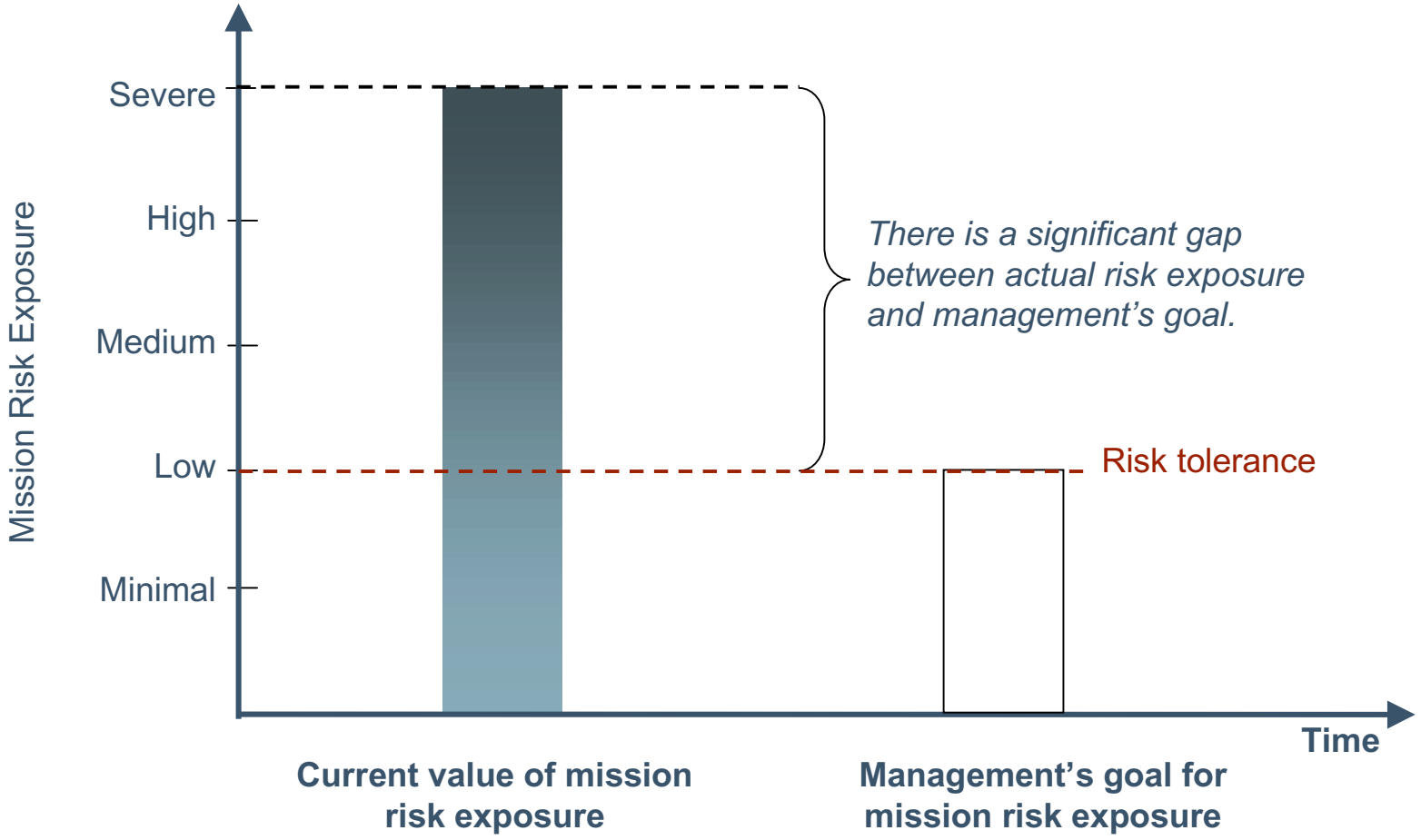
Risk Causal Chain



Combinations of threats, vulnerabilities and controls → **Risk resulting from different operational circumstances** → **Mission risk**

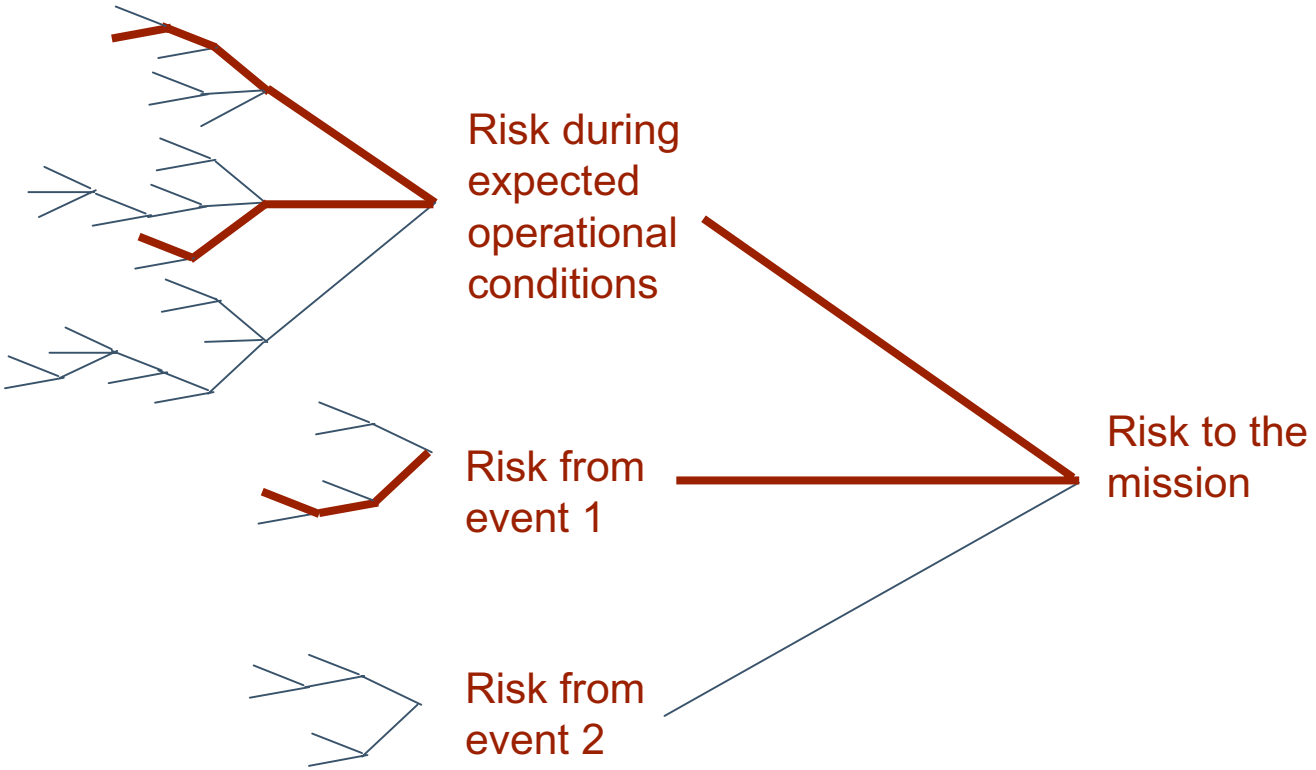
© 2006 by Carnegie Mellon University

Bringing Risk within Tolerance



© 2006 by Carnegie Mellon University

Key Risk Drivers



A critical path analysis identifies the key risk drivers.

© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Protocol Fundamentals - 1

- Determine mission objectives.
- Characterize all operations conducted in pursuit of the mission.
- Define risk evaluation criteria in relation to the mission objectives.
- Identify potential failure modes.
- Perform a root cause analysis for each failure mode.

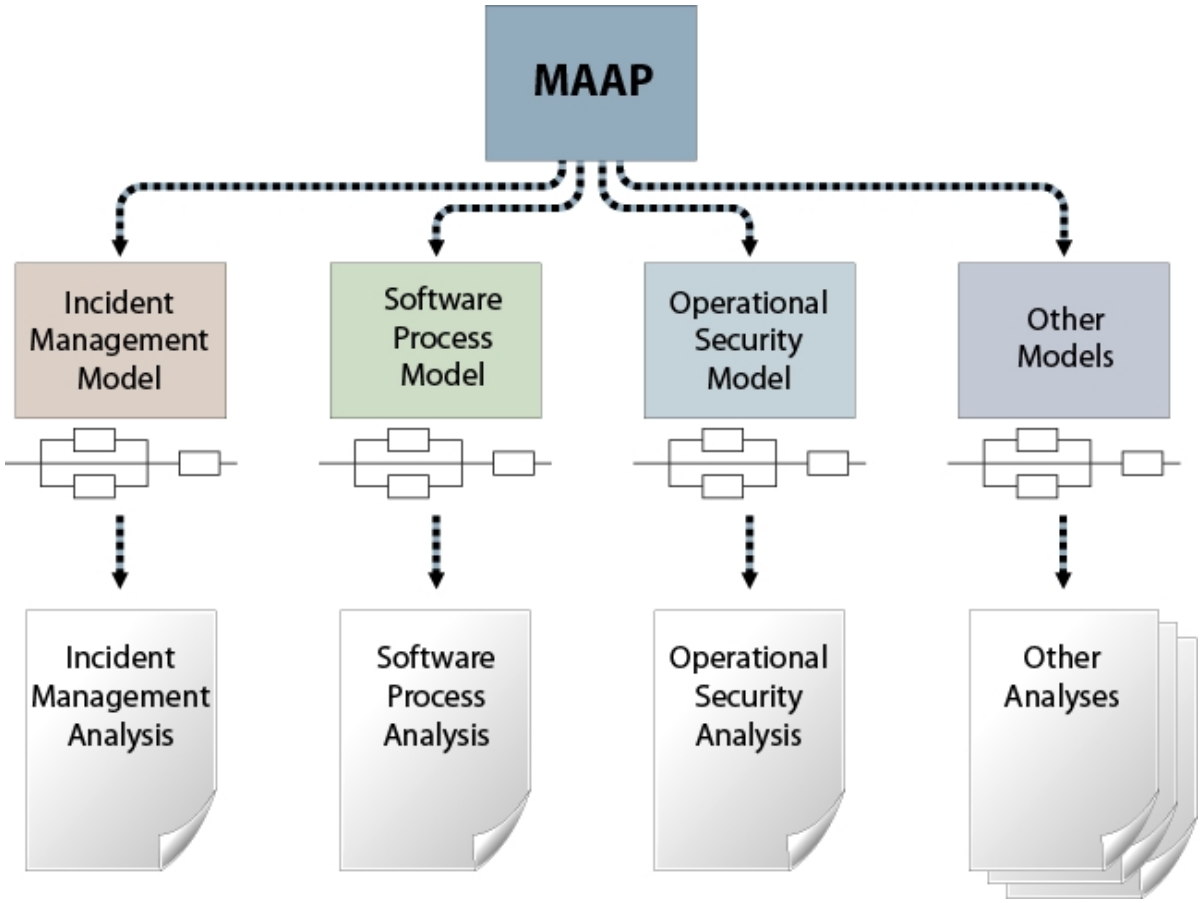
© 2006 by Carnegie Mellon University

Protocol Fundamentals - 2

- Develop a risk profile of the mission.
- Ensure that mission risk is within tolerance.

© 2006 by Carnegie Mellon University

A Common Basis for Analysis



© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

MAAP Pilot

Analyzed an incident management process in a large government organization

Analyzed risk to the mission under normal conditions

- quality of response
- timeliness of response
- customer satisfaction

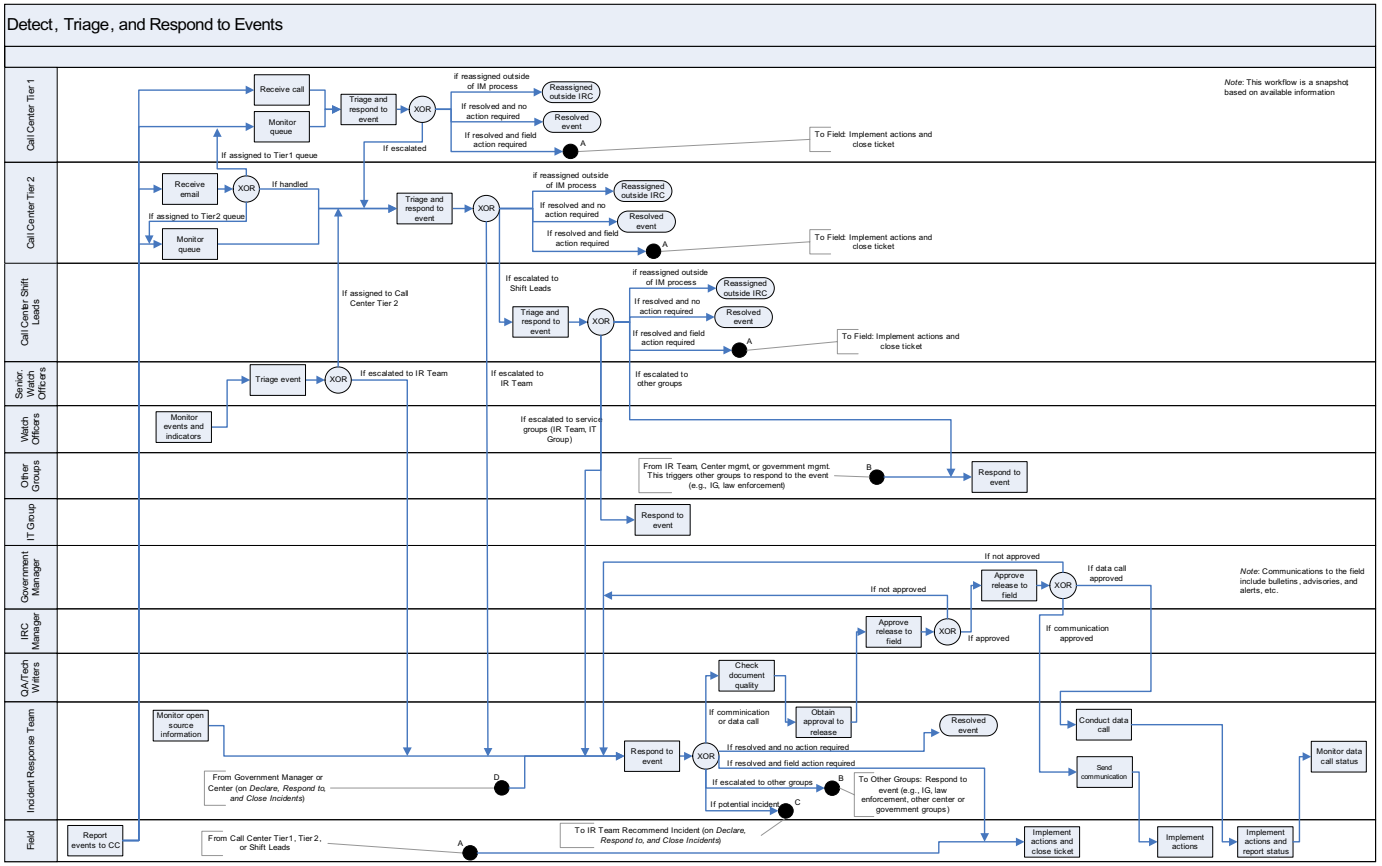
Examined risk to the mission under unusual circumstances

- two major incidents occur at the same time
- cyber security attack renders ticketing system unavailable for an extended period of time

© 2006 by Carnegie Mellon University

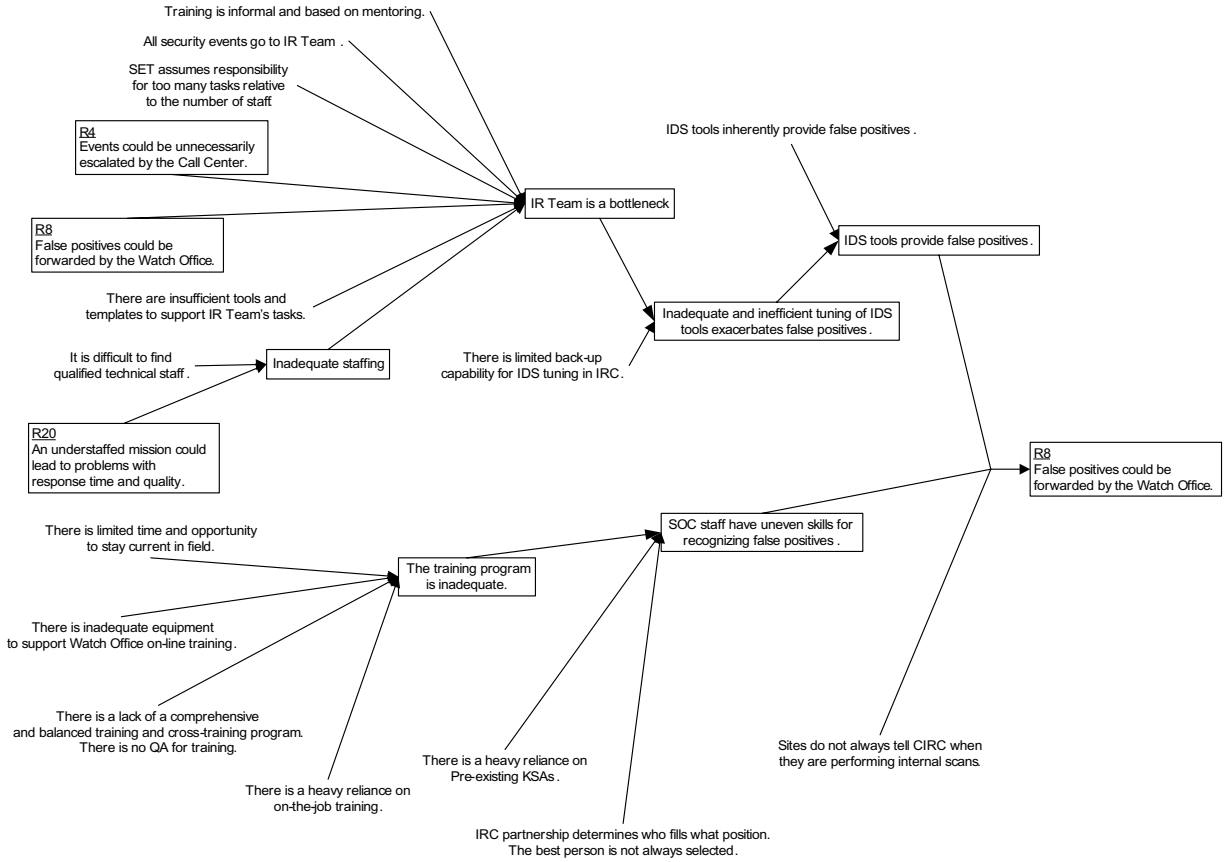
Carnegie Mellon
Software Engineering Institute

Example: Process Workflow



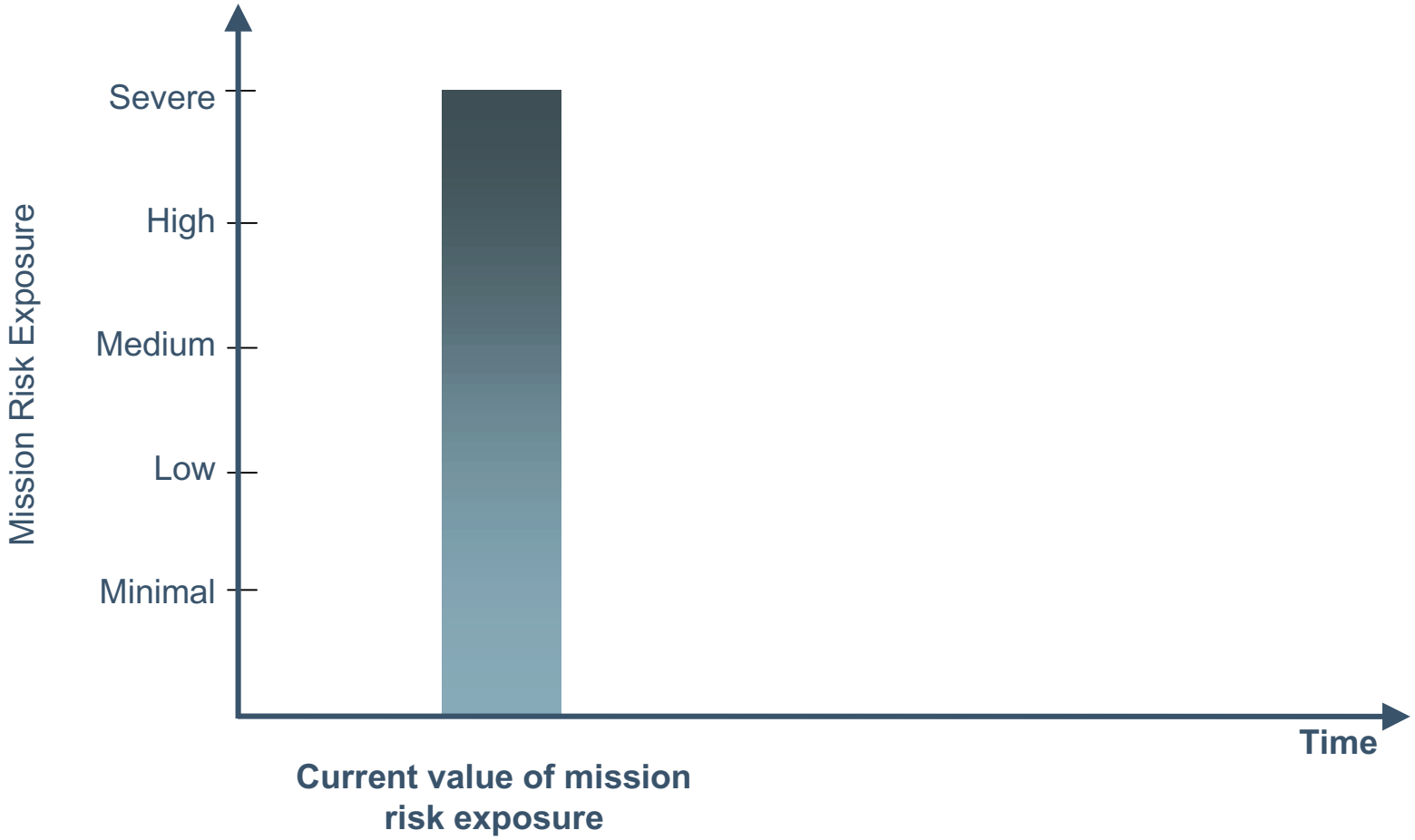
© 2006 by Carnegie Mellon University

Example: Complex Risks



© 2006 by Carnegie Mellon University

Example: Mission Risk



© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

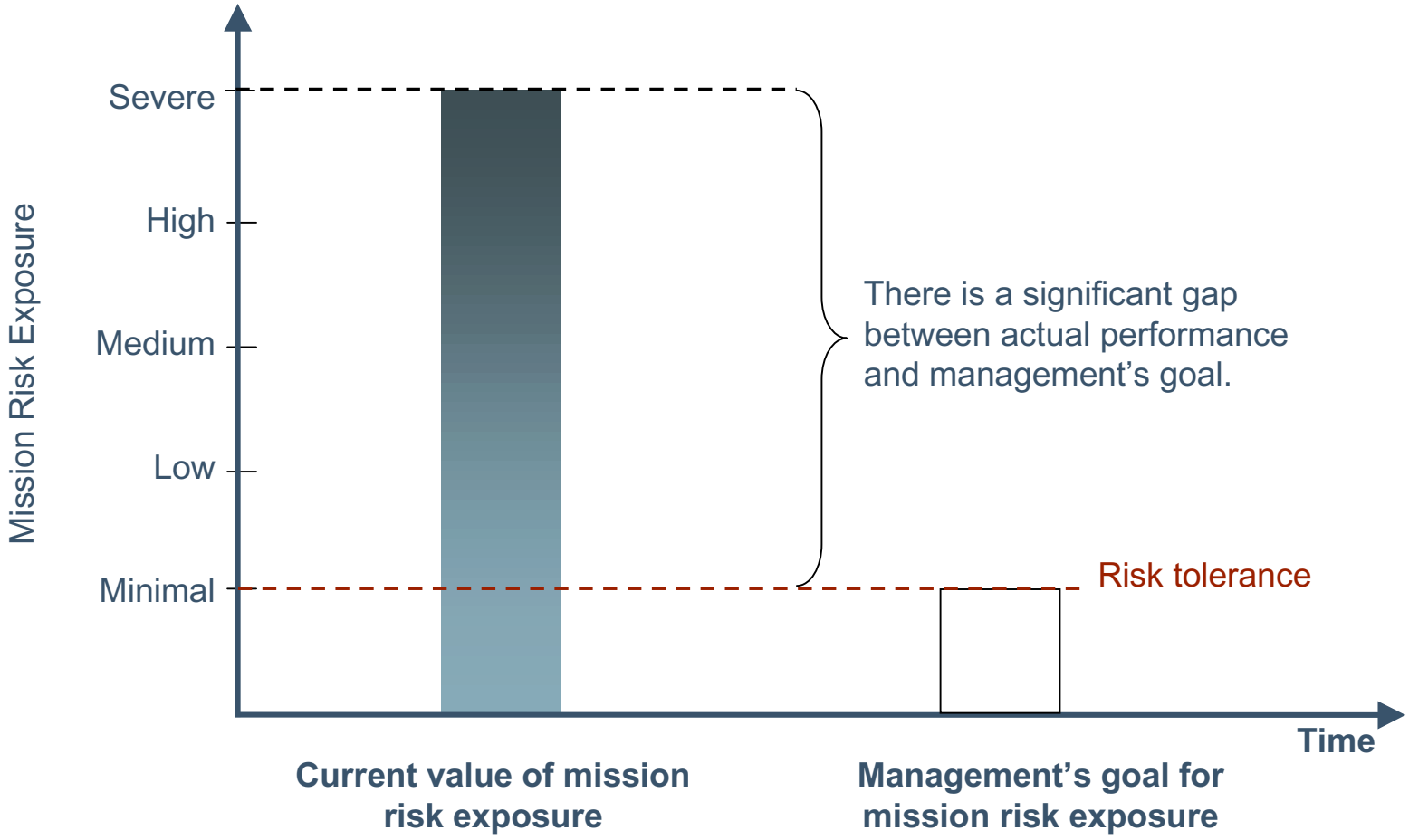
Example: Mission Assurance Goal

Management's goal is to build a "world-class" incident management capability.

This goal translates to very high mission assurance (i.e., very low risk to the mission).

© 2006 by Carnegie Mellon University

Example: Gap in Performance



© 2006 by Carnegie Mellon University

Example: Mitigation Strategy

- Simplify the mission.
  - Determine which incident management services are essential.
  - Develop a plan for growing the incident management capability over time.

- Redesign the process based on the revised mission.

- Develop and test contingency plans.

© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Conclusions

Many types of risk prevalent in today's operational environments (e.g., event risks, inherited risk) are not readily identified using traditional risk analysis techniques.

High-performing organizations have the basic skills needed to identify and manage these new types of risk, but lack sufficient techniques.

Average or poor performers will not have the skills needed to identify and manage new types of risk (and probably have bigger, more obvious risks to deal with).

MAAP is one technique that high performers can use to identify and mitigate the risks arising from operational complexity.

© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Additional Research and Development

Develop a technique for quickly estimating mission risk exposure.

- First pilot will focus on mission assurance in incident management.
- Second pilot will focus on mission assurance in system development.

Refine and document MAAP based on pilot experience.

Pilot MAAP in another domain.

© 2006 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Contact Information

Telephone	412 / 268-5800
Fax	412 / 268-5758
WWW	http://www.sei.cmu.edu/programs/acquisition-support/
U.S. mail	Customer Relations Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213-3890

© 2006 by Carnegie Mellon University