Software Engineering Institute

Survivability Analysis Framework

Robert J. Ellison
Carol Woody

June 2010

TECHNICAL NOTE
CMU/SEI-2010-TN-013

CERT® Program
Unlimited distribution subject to the copyright.

http://www.cert.org



Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Copyright 2010 Carnegie Mellon University.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use. This document may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about SEI publications, please visit the library on the SEI website (www.sei.cmu.edu/library).

Table of Contents

Acknowledgments iv

Abstract v

1 Introduction 1
- 1.1 Background 2
- 1.2 About the SAF Analysis Approach 3

2 The Survivability Analysis Framework (SAF) 6
- 2.1 Analysis Overview 6
- 2.2 Executing the Approach 6
- 2.3 Using the SAF—An Example 7
  - 2.3.1 Selecting and Characterizing Representative Operational Processes 8
  - 2.3.2 Identifying Critical Steps for Analysis 10
  - 2.3.3 Evaluating Failure Causes and Impact 13
  - 2.3.4 Planning Mitigations 14
- 2.4 Variations of the Scenario 14

3 SAF Pilots 16
- 3.1 SAF Pilot: Managing the Scope and Scale of a System Rollout 16
- 3.2 SAF Pilot: Information Assurance 17

4 Value of SAF Analysis 20
- 4.1 Manage Scope of Risk Analysis 20
- 4.2 Include Consideration of Operational Security from the Beginning 20
- 4.3 Avoid Isolated Security Analysis 20
- 4.4 Manage Risks Associated with Interdependencies and Complexity (Expanded Failure Analysis) 21
- 4.5 Incorporate the Effects of Incremental Change 21
- 4.6 Establish a Structured Basis for Risk Reassessments by Documenting Assumptions and Mitigations 21
- 4.7 Establish a Shared View of Security and Survivability 22
- 4.8 Evaluate the Impact of Operational Changes on Mission Survivability in Sustainment 22

5 Conclusion 24

Appendix A: Example—SAF Business Process 25

Appendix B: Reference Tables 33

Bibliography 34

List of Figures

Figure 1: Survivability Analysis Framework 5

List of Tables

Table 1: SAF View of Example, Step A 10

Table 2: SAF Critical Step View with Claims 10

Table 3: SAF Critical Step View with Failure Potentials 11

Table 4: SAF People Summary View for Steps I Through K 12

Table 5: SAF Resource Summary View for Steps I Through K 13

Acknowledgments

There were many who assisted in the development and refinement of this work. Special thanks to Chris Alberts and Ed Morris for assisting in the early development of the approach. Andy Boyd and Morrow Long provided assistance in the development of the connections of SAF to Information Assurance. John Goodenough and Chuck Weinstock worked with us to develop the example we are using in this document and worked with us to connect SAF with a software assurance case.

Abstract

Complexity and change are pervasive in the operational environments of today's organizations. Organizational and technological components that must work together may be created, managed, and maintained by different entities around the globe. The ability of these independently developed pieces to effectively work together after they are built and integrated is uncertain and problematic. The way technology is applied by people to address an operational need must also be understood. Survivability of the organization depends on the capabilities of the people, actions, and technology that compose the operational process to work together to achieve operational effectiveness. A team of Carnegie Mellon University Software Engineering Institute (SEI) software engineers built the Survivability Analysis Framework (SAF) to examine the elements of an operational process and evaluate the survivability and effectiveness of the linkage among roles, dependencies, constraints, and risks to achieve critical operational capabilities. The SAF and the benefits achieved in its pilot use are described in this report.

1 Introduction

The increased complexity of today's widely distributed and highly networked systems and systems of systems[1] exceeds our human capability to understand and effectively validate behavior. Problems with integrating systems are increasingly difficult to identify and fix, particularly when the individual systems were originally designed to run in isolation.

How does one determine if a system or system of systems is sufficient to support an organization's critical mission? Does the technology have sufficient security to meet operational needs? Is the operational result survivable[2]—that is, able to function when there is a disruption in the organization—and reliable for effective operations?

Operational effectiveness frequently requires a well-choreographed flow of people, actions, and technology interactions to successfully address an organizational mission. The interaction among users, hardware, networks, software, and external systems can have unexpected results and potential failures that go beyond each individual system. Failures can arise because of unknown conflicts in the operating assumptions of the various interdependent components. Unfortunately, knowledge of such dependencies and potential failures, many of which are not initially well identified, degrades over time as personnel and operational usage change.

Software is increasingly the largest and most complex portion of a system. In addition, the interoperability of components and interactions among systems is essentially controlled by the software. Software can be highly flexible, but once it is written and implemented it only executes what it has been programmed to do. To appropriately respond to interactions and failures, response behaviors must be designed and built into the software.

Complexity and change are pervasive in the operational environments of today's organizations. Organizational and technological components that must work together may be created, managed, and maintained by different entities around the globe. Net-centric operations and service-oriented

[1] A system of systems (SoS) is a group of interrelated systems that is distinguished from a system by the following characteristics:

- **operational independence of the elements:** Component systems are independently useful.
- **managerial independence of the elements:** Component systems are acquired and operated independently; they maintain their existence independent of the SoS.
- **evolutionary development:** The SoS is not created fully formed but comes into existence gradually as usages are refined, new usages developed, and old usages phased out.
- **emergent behavior:** Behaviors of the SoS are not localized to any component system. The principal purposes of the SoS are fulfilled by these system behaviors rather than component behaviors.
- **geographic distribution:** Components are so geographically distributed that their interactions are limited primarily to information exchange rather than exchanges of mass or energy [Maier 1998].

[2] Survivability is the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.

architectures will push this trend further, increasing the layers of people, actions, and systems that must work together for successful completion of an operational process. Systems and software are not being designed and developed to address this level of dynamic, complex operational interaction. Currently, system design reduction techniques manage complexity by decomposing a system into many simpler components that are essentially constructed in isolation. The ability of these independently developed pieces to be subsequently integrated is uncertain and problematic. Choices made during component development can adversely affect the operational behavior of the integrated system.

This report introduces the Survivability Analysis Framework (SAF)—an analysis technique for analyzing complexity and integration issues throughout the development life cycle. It can be applied at any level of development where the interaction of multiple independently built elements is critical to operational effectiveness. It is designed primarily for project management and stakeholders to ensure that development is proceeding toward an expected operational solution.

1.1 Background

Existing analysis mechanisms do not provide a way to identify missing or incomplete requirements, missing operational considerations, and poorly planned interoperability. Current analysis mechanisms lack the ability to (1) look across multiple systems and organizations to identify integration challenges, (2) consider architecture tradeoffs that carry impacts beyond a single component or a single system, and (3) consider the linkage of technology to critical organizational capabilities. These observations were assembled by a team of software engineers at the Carnegie Mellon University Software Engineering Institute (SEI) based on several years of experience evaluating system and software development and acquisition programs in large governmental military and civil agencies. These observations provide the basis for the work presented in this report.

Another area of research that contributed to the material presented in this report is the SEI's work with the Department of Defense (DoD) on mission threads. The SEI team was asked to consider the effects on increased interoperability enabled by the deployment of the DoD Global Information Grid (GIG) on critical DoD mission threads such as Close Air Support (CAS) and Time Sensitive Targeting (TST). A mission thread can be considered equivalent to an organization's operational process. The initial mission thread analysis identified a gap between theory and practice. The team found that the DoD mission thread documentation represented an "idealized" view of the operational environment; the documentation rarely considered possible failures and often assumed significant homogeneity of computing infrastructure and military hardware. In practice, a successful execution of these mission threads depended on using available equipment and often on ad hoc measures to work around resource limitations. During this research, the SEI team concluded that current analytical mechanisms focus primarily on the technology and only consider the operational execution in selected cases. However, it is the interaction of systems and software with people in the operational environment that is critical to operational effectiveness for technology. Consideration of the technology in isolation is insufficient. The way technology is applied by people to address an operational need must be understood to evaluate operational effectiveness.

In response to these limitations, the SEI team built the Survivability Analysis Framework[3] to examine the elements of an operational process result (people, actions, and technology) and evaluate the quality and effectiveness of the linkage among roles, dependencies, constraints, and risks to determine critical business capabilities. The ultimate goal is to help organizations analyze and understand complex operational processes to determine the impact of issues such as security threats and survivability gaps. In some domains, these processes are referred to as mission threads. We will use these terms interchangeably throughout this document.

The SAF reflects the experience of the SEI team of systems engineers working with real programs to address real problems. It is designed to augment current software and system analysis and development mechanisms to provide the following:

- a means to capture the interactions of software with people and operational actions
- a way to identify and characterize critical operational failure conditions that the technology must be prepared to address
- a way to characterize the realities of the operational context, which should be used for input to the design and development of the technology
- a way to evaluate critical dependencies among people, business or mission outcomes, and technology

We understand the realities of limited time and resources and provide a criticality analysis technique to indicate potential trouble spots that warrant greater analysis when an exhaustive analysis of all possible failure states is not possible. The SAF analysis steps can be repeated at several points in the development and acquisition cycle to evaluate and confirm that the operational context is receiving sufficient attention. This analysis should augment, not replace, existing approaches. The SAF draws from techniques used in risk management, causal analysis, and software assurance, but these have been adjusted to address the challenges of operational complexity.

1.2 About the SAF Analysis Approach

The first step an organization should conduct in an SAF analysis is to construct a well-articulated view of an operational process that documents the interrelationships of people, actions, and technology. This view must be shared by stakeholders and should identify critical steps and the ways in which a step failure could lead to an operational process failure. Analysis of this information provides an opportunity to show how the various parts of technology fit (or should fit, in the case of a planned system) together with the user and organizational aspects to form a repeatable and reliable end-to-end operational process. The SAF provides a structure for gathering and visually displaying the operational process information that can be useful to management, users, technology architects, system engineers, and software engineers.

Operational effectiveness requires an extensive list of components working in harmony.

---

[3] The SAF was piloted for Joint Battle Mission Command and Control (JBMC2) in the analysis of a Time Sensitive Targeting mission thread for the OUSD (AT&L). A second pilot analysis was completed for Time Sensitive Targeting information assurance for Electronic Systems Center, Cryptologic Systems Group, and Network Systems Division (ESC/CPSG NSD).

- hardware—servers, data storage devices, PCs, PDAs, routers, telephone switches, satellite relays, physical access controls, and similar devices
- software—operating systems for each hardware platform, configuration management, databases, firewalls, network protocols, packet switches, authentication packages, web applications, local and remote procedures, and others
- people—organizational roles for system use and support, such as data entry, inquiry, verification, audit, synthesis among multiple information sources, administration for technology components, authentication and authorization authorities, and similar roles
- policies and practices—certification and accreditation, third-party access management, outsourcing contracts, governance controls, and the like

From a pragmatic perspective, the responsibilities for operational qualities such as security and survivability are allocated across all of these components, which must function together to successfully achieve the organizational work process objective. The level of complexity is too high to validate all possible behaviors. Rather, specific scenarios should be developed that characterize how all of the pieces should work together. From these examples, potential weak points can be identified, assumptions about the ways in which components will work together can be verified, and the criticality of each component to the success of the operational process can be evaluated. This analysis is the output of using the SAF. The level of completeness will vary depending on the choice of scenarios. Based on SEI experience, analysis of even a single scenario using the SAF will greatly extend current approaches.

In the SAF analysis, each critical step in an operational mission thread is tasked to fulfill some portion of operational functionality. This tasking represents a "contract" of interaction between each operational step and prior and subsequent steps. Preconditions establish the resources provided to the step. These preconditions may trigger the execution of the step actions (for example, data or a human command), or the actions may be continually executed (such as a sensor). Each step will have outcomes (post conditions) that may interact with subsequent steps. However, the contract with prior and subsequent steps is not necessarily static and may have to be negotiated during execution to reflect changing conditions. Even the identity of prior and subsequent steps may vary across executions of an operational process.[4]

The SAF approach is shown in Figure 1.

[4] Operational processes are expected to be dynamic in content because each specific execution is unique.

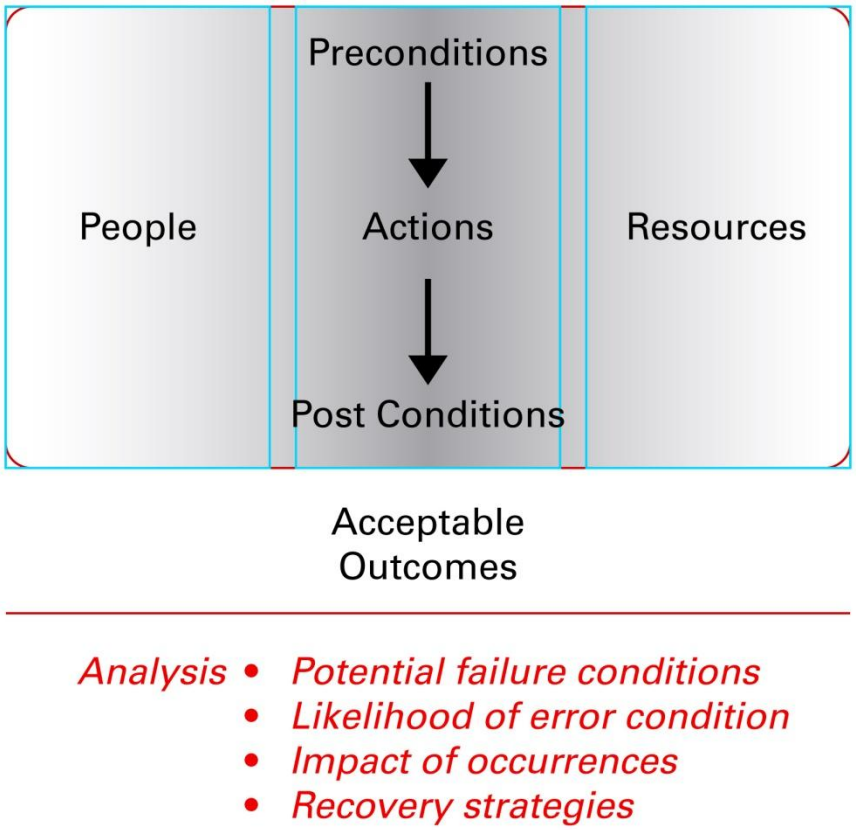


Figure 1: Survivability Analysis Framework

The SAF characterizes the specific actions of each step in an operational process and the linkages between each step (preconditions and post conditions). The details of the SAF and its use through an example are provided in Section 2 of this report.

Section 3 provides insights into two pilot projects where the SAF was applied to consider operational effectiveness and the value that project participants gained. In one pilot, the technique was used to connect information assurance with operational effectiveness. In the second pilot, this technique was used to evaluate the challenges of scale in rolling out a single operational site implementation across a large, highly distributed, multisite organization.

Section 4 summarizes the insights gained by those who used the SAF in a range of pilot projects. Section 5 concludes with a summary of what SAF can provide and why it should be considered for use in complex projects.

2 The Survivability Analysis Framework (SAF)

2.1 Analysis Overview

By using the SAF, organizations can assemble the broad range of information on the people, actions, and technology that must function together in the operational context. The SAF activities, usually performed in the following sequence, are as follows:

1. **Develop one or more scenarios for the selected operational process (end-to-end).**

   Each scenario must include a full end-to-end process (not snippets). The analysis of these scenarios is the primary source of data for the SAF. Scenarios build the knowledge base of the characteristics of the operational context and the supporting systems. A scenario will typically cross many boundaries from start to completion. The scenarios can be current or planned operational processes. Typically the selected scenarios include both current and future processes to describe how new development will fit within the existing operational environment.
2. **Document end-to-end success measures for the operational process.** Document what is expected to happen and the effects if these measures are not met. This is a characterization of the impact of failure on the participating organization(s).
3. **Create a step-by-step SAF flow diagram** for each operational scenario (see the example in Section 2.3). If it is necessary to reduce the scope of the analysis, focus on crucial actions that, if they fail, would have a major impact on operational effectiveness. (This may require preliminary analysis of steps a through d.) Use the flow diagram to
   a. document the collection of external dependencies (preconditions) for each step in the operational process: systems, services, data, policies, connectivity, and people
   b. document assumptions and participant responsibilities as information is exchanged among systems and people (preconditions and actions)
   c. document the expected outcome from each step in the operational process (post conditions and acceptable outcomes)
   d. document the steps that could fail and expected assumptions that may not be met (potential causes of failures)
4. **Identify the failure impact on operational success** for the potential causes of failure (failure outcomes). Consideration should be given to the impact of system failure, resource constraints, communications failure, operator error, or out-of-date information.
5. **Plan mitigations for unacceptable failures.**

2.2 Executing the Approach

The most effective means for applying the SAF is through a series of three types of workshops. The scenarios at the beginning of the workshop series should be high level and idealized, with limited detail. By the end of the series, the scenarios should include a great amount of detail to help participants understand how the pieces in the scenarios will fit together for effective operational results.

The first workshop type, which includes SAF activities 1 and 2, should focus on selection and development of appropriate operational process examples that characterize the current and/or future operational process. A future operational process is what an organization would like to have in place after they have implemented a new operational capability. This type of workshop typically includes 10 to 12 participants from across the development community representing a broad range of roles participating in the development effort, such as architect, software and system engineer, interoperability designer, and tester. Each of these roles can have a different view of the operational context, and it is important to assemble a single shared perspective for analysis. In preparation for this workshop, the facilitators should assemble available use cases into skeleton SAF scenarios to promote discussion. The output from this workshop will include one or more operational process examples that are described in sufficient detail for further analysis and accepted by the participants.

The second workshop type, which supports SAF activity 3, should focus on the operational realities that the operational process must handle. Participants in this workshop must include operational users and operation support resources who currently address the work associated with the selected scenarios. In addition, a subset of attendees from the first workshop should participate. In this workshop, the current and/or planned operational scenarios should be reviewed, and gaps, discrepancies, and limitations for the target operational environment should be identified. Assumptions about the planned operational context should be reviewed and the validity of those assumptions verified.

The third workshop type, which focuses on SAF activities 4 and 5, should include key participants from the first two workshops along with knowledgeable security experts. The focus of this workshop is to identify the impact of potential failures in the scenarios developed in the prior workshops and the effects of such failures on operational success.

Depending on the level of discrepancies identified among participants, each of the three workshop types may require multiple sessions with varying groups of participants to reach a reasonable consensus among the range of stakeholders. For example, if there is too great a gap between the planned and operationally feasible views of the process example, another workshop could be needed to reconcile the discrepancies and build a better example before proceeding to the third workshop type. The workshops could be replaced by individual or group interviews by a team of facilitators, but such an approach requires follow-up reviews with each participant to confirm that the assembled views are realistic and complete.

Developing a well-articulated view of an operational process that is shared by all stakeholders provides an opportunity to uncover differences in understanding, faulty assumptions, and ways in which organizational boundaries could contribute to potential failure. SEI experience has shown that workshop participants learn as much from building the operational process view as from the analysis of it.

2.3 Using the SAF—An Example

Using the SAF requires selection of scenarios that represent the critical operational processes. Each scenario must be decomposed into a series of steps. These steps must represent how the operational process actually occurs for an as-is view or how it is expected to occur for a future perspective. For each step, information about required people, resources, and actions is assembled

in a structured format that accurately portrays who does each action, what initiates the action, what resources are critical to action performance, and the resulting outcomes.

The next section provides an example of the SAF activities using a scenario for a doctor's office ordering tests from a hospital-associated lab.

2.3.1 Selecting and Characterizing Representative Operational Processes

The first SAF activity is to select an important operational process and assemble a general description of the organizational need it addresses and why the process is needed. In this doctor's office example, it is important that lab tests ordered for the patient are performed properly and their results are communicated to the doctor in a timely manner. Early diagnosis of patient conditions before they become critical is a goal for the physicians in this practice. Much of the diagnostic work is outsourced to local laboratories and hospitals. While patients may choose where to have tests performed, in many cases doctors are required to provide referrals. The Health Insurance Portability and Accountability Act (HIPAA) regulations control the sharing of patient identification data with the lab or hospital and the subsequent step of reporting results back to the doctors. The selected multi-organizational operational process example is as follows:

> A patient comes to the doctor for a follow-up visit. This individual was brought to the hospital emergency room several weeks prior with chest pains, treated for a mild heart attack, and released. The doctor, after examining the patient and reviewing the medical history along with the results of tests performed at the time of the office visit, orders further blood tests. Based on the results of these tests, a course of treatment is prescribed and communicated to the patient.

To guide the analysis, it is necessary to clearly articulate the goals of the operational process. What constitutes successful process completion? Many actions may be included that do not directly contribute to successful execution of the end-to-end process and would not warrant in-depth analysis. For this operational process example, the following constitutes success:

- All ordered tests are appropriately performed in a timely manner, and results are accurately communicated to the requesting doctor.
- Patient information is transferred reliably and accurately in a timely manner, with all privacy needs addressed.

The actual sequence of steps required to perform this process is as follows:

A. Patient arrives and checks in for scheduled appointment.
B. Patient's insurance arrangements are confirmed and co-payment is paid.
C. Nurse moves office records and patient into examination room.
D. Nurse takes vitals and electrocardiogram (EKG) (office policy for heart attack patients) and updates office hard-copy records in examination room for doctor.
E. Doctor examines patient and reviews records and EKG.
F. Doctor orders additional lab work.
G. Hard-copy paperwork is returned to medical records unit.
H. Office visit information is transcribed into office electronic medical record.

I. Patient goes to lab for prescribed tests and registers at lab desk.

J. Lab paperwork is prepared and queued for phlebotomist.

K. Phlebotomist takes blood and labels it for lab technician.

L. Lab technician performs tests on sample and generates report.

M. Lab results are transmitted to hospital central repository.

N. Report is transmitted to doctor's office (via email).

For each step in the example, a description of the preconditions, actions, and post conditions must be assembled. People and required resources must be identified. To assemble this view of the operational process, additional information about the context in which the process is performed and its participants is needed. The office context can be described as follows:

- Patient scheduling, electronic medical records, and billing are handled using a package system provided from the hospital (EPICARE), which includes the capability for authorized individuals to link to the hospital database and extract available patient data. The technical characteristics of this system are described in a manual from the hospital. The office has implemented it as a turnkey system with support provided (for a fee) by the hospital vendor.
- Everyone working at the doctor's office has individualized access to the system (nurses, doctors, office clerks, billing clerks, and office manager).
- Administrative control of the office system is handled by the medical records manager (also known as office manager).
- Technical support is provided electronically from the vendor (maintenance, troubleshooting, and upgrades).
- Everyone working at the office has been in their positions for several years.

The lab context is described as follows:

- The LABTEST system is constructed to use the hospital database as an information repository. Patient billing is handled by the hospital. The local office has applications for patient check-in, test paperwork management, results capture from test equipment, and doctor notification.
- Laboratory system actions are streamlined to handle large volumes of input.
- System development and support is handled by the lab group's central office.
- Local administrative support is provided through a contract with the local hospital in conjunction with the database connectivity.
- Staff turnover is high; few workers are in his or her positions beyond a year.

Using the available context information, each step in the process example can be described. Step A is detailed in Table 1.

Table 1: SAF View of Example, Step A

Step A	Patient arrives and checks in for scheduled appointment.
Preconditions	Patient office records are ready at check-in desk. Patient is scheduled for appointment on current date. Doctor has not had emergency requiring schedule adjustments. Check-in access is available to scheduling system.
Actions	Patient is matched to office record file. Patient is flagged as he or she is checked in. Patient demographic data is verified. Patient is given HIPAA form to sign.
Post conditions	HIPAA form is signed. Patient sent to financial window with HIPAA form. Patient file queued for nurse pickup.

The description tables for the remainder of the steps in the medical example can be seen in Appendix A.

2.3.2 Identifying Critical Steps for Analysis

While it is possible to assemble a large amount of detailed information about each step in the process, this activity may not be useful.

A review of the steps critical to meeting the success criteria for the operational process requires focused attention on steps I through M. Of particular concern are steps L and M, where tests are performed and information is transferred from the lab to the doctor's office under the control of a third party (the hospital).

Step I is described as follows:

Table 2: SAF Critical Step View with Claims

Step I	Patient goes to lab for prescribed tests and registers at lab desk.
Preconditions	Patient has an order for lab work. System is in place for collecting patient demographic and insurance information.
Actions	Patient insurance and billing information is collected. Doctor receives report. Medical order is entered into system.
Post conditions	Patient is queued for blood work. Medical order for lab work is properly entered into the system.
Acceptable outcomes	All HIPAA privacy constraints are met. Patient information is accurately input into the laboratory system.

The actions in this step are expected to support the goal for accuracy and privacy of patient information.

For steps of particular concern, potential failures must be considered to identify the ways in which completion of this step could be hampered (failure outcomes). Where possible, provide a link from potential causes of a failure to the operational context. For step L, the description would be expanded as follows:

Table 3: SAF Critical Step View with Failure Potentials

Step L	**Lab technician performs tests on sample and generates report.**
Precondition	Blood and paperwork are ready. Technician loads proper machine with blood sample. Bar code on vial indicates patient and proper test to machine.
Action	Machine runs tests. Each machine sends results to lab's database collection point. Results are collated into report for transmission to the hospital repository.
Post condition	Report exists. Blood is disposed of properly. Technician performing work is identified and linked to results.
Acceptable outcomes	All required tests were run. No unordered tests were run. Test results are accurately recorded. Test results are associated with the right patient. Lab audit trail exists—who did the work, who was the operator, and so forth. Access to results meets HIPAA requirements, such as technician's inability to identify the patient associated with the test results.
Failure outcomes	Missing (or delayed) results • Some or all tests are not done. • Some unrequested tests were performed. Wrong results • Results do not reflect the actual sample. Disclosure • Results are disclosed to unauthorized person. • Test results are not associated with the correct patient. • Test results are not associated with the correct doctor.

(*Continued*)

Table 3: SAF Critical Step View with Failure Potentials (cont.)

Step L	**Lab technician performs tests on sample and generates report.**
Potential causes of failure	Missing results • Paperwork requiring tests to be run was lost or misplaced. • Blood samples were lost, contaminated, or misplaced. • Some tests were not run by the technician. • Wrong tests were run by the technician. • Some or all test results were not associated with the correct patient (in the lab). • Some or all test results were not associated with the right doctor (in the lab). • Lab database was inaccessible for receiving results. • Machine did not produce results. • Machine was not working and could not produce results. Wrong results • Machine doing the test has an undetected internal failure so results were produced, but they are not the correct results. • Analysis machine is not calibrated, has faulty reagents, or similar faults. Disclosure • Unauthorized entity (person, insurance company, or others) gained access to the analysis results during analysis (in the lab).

Two summary views (simplified versions of RAM[5] matrices) shown in Table 4 and Table 5 focus attention on people and resources. The people view (Table 4) identifies roles involved in each step. If it is known, the controlling role (decision maker) for each step is noted so shifts in responsibility as well as organizational shifts can be visually articulated. Such shifts represent a change in governance and policy that can lead to a process failure. The controlling role is marked as *C*, and participants are marked as *X*.

Table 4: SAF People Summary View for Steps I Through K

	I) Patient to lab	**J) Lab paperwork prepared**	**K) Blood sample drawn**
Patient	X		X
Lab check-in staff	C	C	
Phlebotomist			C
Lab technician			

Resources for steps I through K are identified in Table 5 (the controlling role is marked as *C*, and participants are marked as *X*).

[5] A responsibility assignment matrix can include those responsible, those with decision authority, those who are consulted, and those to be informed. See http://en.wikipedia.org/wiki/Responsibility_assignment_matrix.

Table 5: SAF Resource Summary View for Steps I Through K

	I) Patient to lab	J) Lab paperwork prepared	K) Blood sample drawn
Lab work order	X	X	
Patient insurance data	X		
HIPAA forms	X		
Lab scheduling	X	X	
Lab test repository and reporting system			
Blood sample			X
Lab paperwork (labels)		X	X
Testing machine			
Testing machine connectivity			
Doctor's office connectivity			

For a complex operational process, resources should be assembled in groups based on the way those resources are managed: resources controlled by a specific organizational unit would be grouped together. For example, resources controlled by the doctor's office would be grouped separately from those controlled by the laboratory or other third-party contractors. This provides visibility to potential variations in governance (policy) and allocation models (such as service level agreements) that could impact performance of the operational process.

The full people and resource tables for steps I through M of the medical example are provided in Appendix B.

2.3.3 Evaluating Failure Causes and Impact

Evaluating failure opportunities requires looking across the information collected for each step and identifying what could happen when something does not function as intended. In addressing this activity, select a critical step and consider each precondition, action, and post condition to identify meaningful ways failure could occur. Build on failures that have already occurred in current operations. These provide indications of variability that need to be handled. When identifying failure for an operational process that does not yet exist, evaluate mitigations currently in place to determine how the conditions that trigger the need for the mitigation will be handled in the changed operational context.

Unexpected errors and variations that the operational process is not designed to accommodate can occur, leading to failure of a critical step and subsequent impact on the successful completion of the operational process. In building the failure outcomes for each critical step, a range of potential failures should be considered.

Operational process failures can be caused by changes in usage as well as traditional causes such as hardware failures. Failures frequently arise from a combination of errors that when considered individually would not lead to a failed state. Using our medical example, a test equipment failure can delay test results for a significant number of patients. The delays temporarily reduce the available capacity to deal with other events. The occurrence of an additional problem such as transmission problems to the hospital database, combined with limited storage capacity for data at the lab, could lead to lost test results.

Options for failure causes (Potential Causes of Failures) may include

- interaction- (data-) triggered failures—missing, inconsistent, incorrect, unexpected, incomplete, unintelligible, out of date, duplicate
- resource-triggered failures—insufficient, unavailable, excessive latency, interrupted access
- people-triggered failures—information overload, analysis paralysis, distraction (rubbernecking), selective focus (only looking for positive reinforcement), diffusion of responsibility (for example, "It's not my job."), lack of skills or training

Discrepancies arise normally in operational processes. The overall success of a process depends on how effectively discrepancies are accommodated through the people, resources, and actions that compose the end-to-end process. Changes in operational processes and systems can introduce new types of discrepancies. For example, a system that was developed for a local facility but is now supporting a process distributed across multiple sites may require revision to accommodate the increased complexity of information interchange. Dealing with discrepancies becomes much more difficult as the number of participants—people and systems—increases. Each participant has to deal with multiple sources of discrepancies, and a single discrepancy can affect multiple participants. A system failure can affect multiple organizational processes.

2.3.4 Planning Mitigations

Further analysis may be needed to identify which failure outcomes are sufficiently critical as to require mitigation. Mitigations may already be in place; these should be verified against the potential failures to verify their appropriateness.

For example, if the organization must report any unauthorized disclosure to the affected individual, disclosure failures that represent a major organizational cost and avoidance of the failure should be considered. If a failure to run a test is considered critical, the organization may wish to invest in more tightly coupled electronic communication between the doctor's office and the laboratory. However, addressing one type of failure could potentially create others. In the doctor's office example, an electronic communication between the doctor's office and laboratory could fail, resulting in the loss or delay of all tests. This communication link could also be maliciously compromised, resulting in disclosure of data, and a separate verification channel may be needed.

2.4 Variations of the Scenario

The doctor's office scenario described in the sections above could represent the current operational process. There could be a technology change proposed to give the doctors handheld devices for ordering tests and providing them with access to patient information. This would change how step G is described. Availability and connectivity of the handheld device would be an

additional prerequisite as well as the doctor's access to the device and to the patient information through the device. Protection of the patient's information on the new device and in the transmissions between the device and the receiving point for the lab requests would be needed. In addition to the selection of a usable device with the features and functions desired, the availability and information protection needs become additional requirements that must be considered in the selection process. Also there are several ways the operational process could be adjusted to accommodate the new device. Will the central medical unit continue to collect a hard copy of the information for monitoring, or will that information be transitioned to a repository? How will the handheld device interface with each of these options? Different failure outcomes result from the various choices, and these can be analyzed and compared if each changed step is described using the SAF template structure. The discussion of these and other questions with stakeholders in the workshops provides an opportunity to clarify operational expectations and identify gaps.

Another change could involve the hospital shifting their central repository to cloud technology to reduce costs, which may require each doctor's office and laboratory to change its access. By evaluating the change using the SAF, changes in the failure potentials and security implications can be identified. Unexpected consequences can be identified, and plans can be changed or additional mitigations put in place as needed.

3 SAF Pilots

In practical execution, no organizational process is static. There are adjustments due to limitations of available resources and the need to consider the interaction of systems and software with people. How well can an operational process tolerate the following operational realities?

- Operational processes require integrating system and people actions across a constantly evolving mix of systems and people.
- Increased reliance on shared technology/services requires establishing operational trust among systems, software components, and services.
- Establishing and maintaining operational processes requires traceability between technical decisions and business requirements.
- Operational processes need to allow for adjustments to meet immediate, critical needs. This flexibility contributes to their fragility.

When the SEI team used the SAF on pilot projects, we noted similarities in the failure analysis of operational processes across many organizational domains. How well can the current and/or planned operational process accommodate the following discrepancies, and how could a failure affect that process?

- Operational process breakdowns can arise from a combination of failures that drive operational execution outside of acceptable limits.
- Work processes span multiple systems, and a failure of one system can affect the overall work process within that system and within other participating systems.
- Systems developed at different times have variances in technology and expected usage that become problematic, especially as a system is extended and repaired.
- Human interactions may be necessary to connect systems. This can result in the erosion of the people/system boundary as people become an integral part of the system.

The SAF has proved to be an extremely flexible technique that supports analysis needs for operational effectiveness in a broad range of projects at varying points within the life cycle. It can be applied at any level of development where the interaction of multiple independently built elements is critical to operational effectiveness. The SAF provides a way to raise and evaluate the operational realities and failure potentials that can plague operational effectiveness. The two examples selected for this section give a sample of the range of analysis that can be addressed.

3.1 SAF Pilot: Managing the Scope and Scale of a System Rollout

The SAF was applied to the development of a medical scheduling system. Medical services were delivered at multiple sites, with each site scheduling its own services. An objective for the new system was to provide a distributed scheduling capability to better balance resource loads and to simplify appointment scheduling for patients. A patient representative would be able to schedule appointments at multiple locations.

An objective for the SAF analysis was to increase management understanding of the effects of the distributed capability so that the effects of its deployment and the future effects of decisions were better understood. The existing analysis had not fully considered the effects of the scale of the rollout and the interactions of legacy and new work practices.

Some of the SAF benefits observed during the workshops included the discovery of the following needs:

- A description of actions that may be required should be given to management.
  - An insufficient level of flexibility of a new system was identified after considering how an operational process must differ among sites for a multisite, distributed organization.
  - Primary care is scheduled differently from specialty areas and should be evaluated independently.
  - Variations in operational impacts were identified and evaluated after the proposed operational process from the perspective of a range of users was considered. For example, in a hospital environment the impact of a change can vary greatly among patients, medical personnel, and administrative users.
- A list of operational process risks for a distributed system should be based on analysis of a representative set of sites. The primary focus of risk management had been on project schedule and costs with the scope of that analysis limited to a single site.
  - Site planning for the rollout required identifying gaps among provided and expected functionality, the impact of bringing faulty data into the new system from the legacy system, the range of people that could be affected by the transition (not just schedulers), and critical organizational issues at individual sites that could hinder the transition.
  - It was not clear how the proposed system could accommodate fee services that are purchased externally from local providers and how these services would be linked to the patient schedule.
  - Scheduling did not have an enterprise owner; no single area had the responsibility for providing effective scheduling.
- A template of examples should be provided that could be used as a planning tool to identify gaps that arise from site-specific issues such as training and system configurations.

3.2 SAF Pilot: Information Assurance

Several SAF pilots involved information assurance for systems of systems. An operational process that operates across multiple sites has to manage significant variations in available computing resources and operational threats. Systems are deployed and upgraded at different times. There may be security policy conflicts among sites in terms of the accepted ports and protocols and wide variations in operational capabilities. The DoD central command locations, for example, have robust communication resources, while networking for combat units (referred to as the tactical environment) may have a less reliable networking capability based on line-of-sight radio links.

Strategic planning documents like The Department of Defense Information Assurance Strategic Plan [DOD 2009] anticipated the need for end-to-end information assurance (IA) requirements and declared strategic goals to apply to all levels. However, those goals do not address the

operational differences. The IA services proposed as sufficient for the central command locations may not be effective or applicable for the tactical edge of the network. The SAF IA pilots concentrated on analysis of the tactical operational environment.

The SAF had to be augmented for these pilots to cover possible risk mitigations, an IA requirement. The primary change was to add a step called *Determine Failure Types*. There are a variety of ways that failures can be organized. Failure or threat types can be based on effects. For example, availability, integrity, and confidentiality are frequently the threats types for security. Failures and threats can also be organized in terms of the target, such as communications, users or operators, policies, data storage, infrastructure services, and applications. External system failures cannot be mitigated by prevention but rather by mitigations that bound the effects of such failures or support effective recovery mechanisms.

The following issues were considered by the SAF analysis:

- How should the IA services deal with sporadic connections? There is a significant risk that IA failures in the tactical environment become a denial of service for the operational mission that is technology dependent. Currently technical support personnel often resolve communication problems. When processing involves multiple systems with more complex IA controls, manual intervention seems less likely to be successful. It is difficult for a local operator to identify the cause of a failure, which, given the ad hoc nature of a tactical environment, may have been generated by another unit or by operating conditions, such as terrain or weather, that affect radio communications. Recovery could be complicated by independent actions taken by each affected unit.
- Failure recovery had to be considered in the context of the operational mission. Often a communication resource such as a unit that is relaying messaging is supporting multiple mission threads, and network quality of service decisions have to consider relative mission priorities.
- In planning for changes to mission critical resources, the analysis of IA threats can provide insight into additional capabilities that are needed to ensure mission thread success. One example required consideration of quality of service, dedicated channels, and image resolution analysis to mitigate the impact of the bandwidth constraints that could lead to mission failure if the planned image data did not reach its target destination. These considerations must be balanced with the IA mechanisms, such as encryption and enclave barriers, that can reduce the available bandwidth. The SAF analysis provided a way to articulate choices for IA, mission connectivity, and other resources and identify application requirements that more effectively supported the success of a mission.

The following example describes how SAF is applied to IA for proposed technology changes. The mission *Close Air Support* typically involves an Air Force aircraft supporting an Army ground unit. More extensive interoperability is possible as analog radios are replaced by digital units that support wireless Internet Protocol networks. Such connectivity could provide ground forces with better access to real-time situational information, but the additional dependencies introduced by a net-centric operating environment can fundamentally change how participants analyze and respond to failures. In one specific situation, a sensor on an Army ground vehicle provided information used locally by personnel in that vehicle, but that information may also have been critical for a mission that involved an air strike. Prior to the SEI team's involvement, technology

changes had been proposed for extensive data sharing. Several kinds of failures or changes could arise from that proposed technology change: sensor failure, radio failure, software failure that requires a restart, changes that affect priority given to computing processes executing on that vehicle that create unacceptable data latency for the mission, changes in vehicle location that disrupt wireless communications, or vehicle occupants' changes in sensor configuration to mitigate a risk to them that then degrades the sensor information for the mission. The SAF was used to assemble potential failures of IA, mitigations, and mission impact to identify gaps and evaluate the mission operational effectiveness of planned IA measures.

4 Value of SAF Analysis

The SAF provides a foundation of content that can be connected to other analysis techniques to provide a broader basis for decision making. The SAF provides a top-down perspective that is readily grasped by acquisition and management. Through extensions that connect the SAF to other analysis techniques, specialists can integrate their greater detail into the broader perspective.

The SAF provides a structured way to identify and document the connections among people, actions, and technology in the operational context. By assembling a shared view of critical operational processes and embedding the view with operational reality, management can identify connections and gaps that are not visible in the current techniques applied for system and software development. The information assembled in the SAF supports traceability between technical decisions and business requirements and serves to identify gaps between operational assumptions and operational realities.

By focusing on the operational realities of an operational process, the SAF provides a means to move outside of the idealized and desired result to identify the assumptions, limitations, and potential failure opportunities. An operational process must be able to tolerate discrepancies, but nothing can be constructed to tolerate all possible problems. The SAF provides a means to look beyond each individual component to identify how well the whole can function.

4.1 Manage Scope of Risk Analysis

Limited resources are always a constraint. The SAF addresses those constraints in several ways, but the analysis does not attempt to be complete. The first activity in the SAF process concentrates on identifying representative operational contexts that raise significant issues. The identification of issues provides a motivation to analyze further as needed.

4.2 Include Consideration of Operational Security from the Beginning

The SAF provides a way to include the consideration of the target operational context from the beginning of a development effort. Typically these considerations do not receive attention until a project nears completion, which is when the opportunity for adjustment to significant issues is extremely limited. The techniques used by the SAF can be applied at any point within the life cycle for consideration of complex issues such as security and survivability.

4.3 Avoid Isolated Security Analysis

Analysts typically decompose complex software problems, but decomposition by components or by system attributes such as performance, reliability, or security typically scatters the knowledge across multiple development units and a diverse group of experts. For example, security analysis often concentrates on certification and accreditation, but such a focus can miss essential connections among security, the implementation of the system's functionality, system interoperability assumptions, and operational constraints.

The diffusion of information and analysis compounds management decisions. The SAF was applied initially to security and survivability, as those risks and mitigations are often not expressed in terms that management could evaluate or that supported effective operational tradeoff analysis. The diffusion of information and analysis is particularly evident for a system of systems where the individual systems do not share common management and have differing risk profiles. A shared view, constructed through the SAF analysis, provides a focal point for discussion among the various component stakeholders to reach a workable consensus.

4.4 Manage Risks Associated with Interdependencies and Complexity (Expanded Failure Analysis)

The analysis of failure of an operational process and the ways an organization would be impacted could

- determine what to monitor
- identify dependencies among infrastructure, organizational processes, and application systems. Are there inconsistent operational assumptions among systems that could lead to a failure? How do those dependencies constrain change management for each of the systems or for the operational process?
- consider the effects of a shift of control for the computing assets that support an operational process. For example, mobile computing devices can be controlled by the user and in some instances by a corporate host.
- identify design assumptions that could be challenged by changes in the supported work processes

4.5 Incorporate the Effects of Incremental Change

The SAF's initial focus on survivability was motivated by the concurrence of changes from multiple sources: system-of-system constituents, technology infrastructure, business requirements, operational work processes, new attack patterns, and new software vulnerabilities. Such changes can affect the behavior of a system of systems by introducing new functionality or by incorporating interfaces to additional systems. As a result, these changes could provide new opportunities for an attacker, create new failure states, and complicate failure analysis and recovery by changing what had been considered normal behavior. While each one of a series of incremental changes can appear to be straightforward, over time, such changes can invalidate previous risk assessments. By looking across the operational process using the SAF, the operational and organizational impact of small changes can be better determined. Small changes with localized impact can be handled at the component level, and management attention can be focused on changes with far-reaching implications. In current situations, implications beyond cost and schedule are infrequently articulated appropriately to management, and the operational impact comes as a surprise.

4.6 Establish a Structured Basis for Risk Reassessments by Documenting Assumptions and Mitigations

As time passes and personnel change, an understanding of operational assumptions and design decisions made to address identified risks is often lost. Retaining this understanding is particularly

important for systems of systems where the expected behavior of external systems also has to be understood. Information about the assumptions and limitations of the technology is usually buried within the details of voluminous design and development documents. Such documentation can be useful when a reassessment is required; this information needs to be accessible to the stakeholders. The documentation has to cover more than the technical issues. Operational effectiveness requires an understanding of the connections among people, systems, applications, infrastructure, and business functionality. The SAF can be used to assemble this operational perspective.

4.7 Establish a Shared View of Security and Survivability

Elements of security and survivability are scattered across the many disciplines that work together in addressing system and software development. Bodies of work that consider portions of security and survivability may be available from continuity of operations, natural disaster response, vulnerability management, and so on. For example, architecture analysis often uses scenarios or analyzes data flows, which are extracted from the work process. Use cases are frequently applied, but they focus primarily on the technology without effectively considering the individual actors using the technology within the operational context. Organizations conduct failure analysis, which leads to abuse cases that are considered by system and software engineers. These cases are not always addressed in the same manner by the different disciplines involved.

The SAF helps to construct a well-articulated view of an operational process that is shared by all stakeholders. This view provides an opportunity to uncover differences in understanding, faulty assumptions, and ways in which organizational boundaries could contribute to stress and potential failure.

Determining the critical steps and the failure outcomes can require the active participation of many stakeholders, including operational process owners, functional and informational subject matter experts, and operational resources knowledgeable about the organizational technology infrastructure. This brings together a range of knowledge that is usually broadly dispersed in the organization among people who have limited, if any, interaction. Though the steps to construct this shared view can be time consuming, drawing this dispersed information together in a shared view allows all organizational participants to understand their roles in the process and the ways in which the choices they make affect others.

The long-term value in assembling shared views of important operational processes is the ability to consider the effect of change on operational success over time. With the availability of a shared view that includes the full range of interactions, the impact of change can be expressed as its effect on the people, actions, and resources that make up the operational process and contribute to its ongoing success. Proposed changes to an operational process can be evaluated to determine potential problems for operational success and requirements for effective mitigation.

4.8 Evaluate the Impact of Operational Changes on Mission Survivability in Sustainment

With the availability of a shared view, proposed operational changes can be evaluated as to the impact they will have on operational process success. Currently, limited information about the operational processes flows to the operational sustainment resources. The shared views developed

from the SAF can provide a rich basis for including consideration of operational qualities beyond cost and operational resources.

5 Conclusion

Organizations will continue to increase their dependency on systems and systems of systems, and this change will continue to escalate in technology. As the systems evolve, new technology must interoperate with existing operational environments. This complexity requires the use of analysis techniques that provide a shared view of multiple layers of interdependency. Information needed to assemble the shared view must be drawn from a broad range of participants and components at many organizational levels.

A number of trends compound the difficulty of achieving and sustaining operational work processes.

- Technologies such as web services make it easier to assemble systems, but ease of assembly may only increase the risk of deploying systems with unpredictable behavior. Fairly simple computing architectures that could be understood have been replaced by distributed, interconnected, and interdependent networks. Business requirements increase the likelihood of failure by bringing together incompatible systems or by simply growing beyond the ability to manage change. As we depend more on interdependent systems, failures are not only more likely but also more difficult to identify and fix.
- An increasing number of failures are caused by unanticipated interactions between system-of-systems constituents. Failures may be the result of discrepancies between the expected activity and the actual behavior that occurs normally in operational processes. The overall success of an operational process depends on how these discrepancies are dealt with by staff and supporting computing systems. Changes in operational processes and systems often introduce these kinds of discrepancies.
- Dealing with discrepancies becomes much more difficult as the number of participants—people and systems—increases. Each participant has to manage multiple sources of discrepancies, and a single discrepancy can affect multiple participants. There is increased likelihood that a poorly managed discrepancy will result in additional discrepancies affecting additional participants. Failures are frequently the result of multiple, often individually manageable errors that collectively become overwhelming.

The SAF provides a way to incorporate multiple perspectives—among systems, organizational units, operational processes, and roles. With this shared view, integration tradeoffs and failure potentials can be identified and addressed throughout the life cycle to improve qualities such as security and survivability.

Appendix A: Example—SAF Business Process

Business Process Example

A patient comes to the doctor for a follow-up visit. This individual was brought to the hospital emergency room several weeks prior with chest pains, treated for a mild heart attack, and released. The doctor, after examining the patient and reviewing the medical history along with the results of tests performed at the time of the office visit, orders further blood tests. Based on the results of these tests, a course of treatment is prescribed and communicated to the patient.

Business Process Steps

A. Patient makes an appointment for an office visit to follow up on hospital release.

B. Reminder is sent to patient about scheduled office visit.

C. Patient's available records are assembled for use in office visit.

D. Patient arrives and checks in for scheduled appointment.

E. Patient's insurance arrangements are confirmed and co-payment is made.

F. Nurse moves office records and patient into examination room.

G. Nurse takes vitals and electrocardiogram (EKG) (office policy for heart attack patients) and updates office hard-copy records in examination room for doctor.

H. Doctor examines patient and reviews records and EKG.

I. Doctor orders additional lab work.

J. Hard-copy paperwork returned to medical records unit.

K. Office visit information is transcribed into office electronic medical record.

L. Patient goes to lab for prescribed tests and registers at lab desk.

M. Lab paperwork is prepared and queued for phlebotomist.

N. Phlebotomist takes blood and labels it for lab technician.

O. Lab technician performs tests on sample and generates report.

P. Lab results are transmitted to hospital central repository.

Q. Report is transmitted to doctor's office (email).

R. Doctor reviews test results and develops treatment plan for patient.

S. Treatment plan is communicated to patient.

Business Process Context

The office context can be described as follows:

- Patient scheduling, electronic medical records, and billing are handled using a package system provided from the hospital (EPICARE), which includes the capability for authorized

individuals to link to the hospital database and extract available patient data. The technical characteristics of this system are described in a manual from the hospital. The office has implemented it as a turnkey system with support provided (for a fee) by the hospital vendor.

- Everyone working at the doctor's office has individualized access to the system (nurses, doctors, office clerks, billing clerks, and office manager).
- Administrative control of the office system is handled by the medical records manager (also known as office manager).
- Technical support is provided electronically from the vendor (maintenance, troubleshooting, and upgrades).
- Everyone working at the office has been in his or her position for several years.

The lab context is described as follows:

- LABTEST system is constructed to use the hospital database as an information repository, and patient billing is handled by the hospital. The local office has applications for patient check-in, test paperwork management, results capture from test equipment, and doctor notification.
- Laboratory system actions are streamlined to handle large volumes of input.
- System development and support is handled by the lab group's central office.
- Local administrative support is provided through a contract with the local hospital in conjunction with the database connectivity.
- Staff turnover is high; few workers are in their positions beyond a year.

SAF Step Descriptions

Each step describes preconditions, actions, and post conditions to fully characterize the interaction of people, actions, and technology that must occur to complete each step.

Step A	**Patient makes an appointment for an office visit to follow up on hospital release.**
Preconditions	Patient requires follow-up doctor's visit for hospital stay. Appointment staff has appropriate authorization for scheduling, doctor availability, and patient demographic information. Telephone and computer system are available.
Actions	Patient calls doctor's office. Appointment staff answers phone. Appointment staff accesses, verifies, and updates patient contact information as needed. Appointment staff accesses doctor's schedule. Appointment date and time are selected and updated with patient agreement. Appointment is flagged as follow-up to hospital stay.
Post conditions	Appointment notification is scheduled for day before appointment. Appointment is scheduled and in the system for proper patient, date, time, and doctor.

Step B	Reminder sent to patient about scheduled office visit.
Preconditions	Appointment is scheduled for the next day. Valid patient phone number is available to scheduling system. Recorded message is set up for appointment reminder service.
Actions	Scheduling system dials contact number and sends recorded message linked to appointment date and time.
Post conditions	Call made to number on file with the appropriate information.

Step C	Patient's available records are assembled for use in office visit.
Preconditions	Patient is scheduled for appointment on current date. Appointment is flagged as hospital visit follow-up. Medical records department has access to hospital patient records.
Actions	Medical records performs the following: • Patient is matched to proper records: electronic and paper files (some identifier). • Office files are pulled for use. • Hospital data (discharge summary) are extracted from hospital database into office electronic record and printed.
Post conditions	Office electronic record is updated with hospital information. Hard copy is updated for office visit use.

Step D	Patient arrives and checks in for scheduled appointment.
Preconditions	Patient office records are ready at check-in desk. Patient is scheduled for appointment on current date. Doctor has not had emergency requiring schedule adjustments. Check-in access is available to scheduling system.
Actions	Patient is matched to office record file. Patient is flagged as he or she is checked in. Patient demographic data is verified. Patient is given HIPAA form to sign.
Post conditions	HIPAA form is signed. Patient sent to financial window with HIPAA form. Patient file queued for nurse pickup.

Step E	Patient's insurance arrangements are confirmed and co-payment is made.
Preconditions	Patient is standing at finance window. Patient has valid insurance card. Co-pay required (optional). Access to scheduling system and patient electronic record is available. Access to insurer's data about the patient coverage is available.
Actions	Insurance information is validated in patient's electronic record. Co-pay is collected (if required), and scheduling system is tagged with payment.
Post conditions	Insurance information for patient is validated. Patient is registered for appointment with co-pay (if required).

Step F	Nurse moves office records and patient into examination room.
Preconditions	Patient office records are queued for nurse. Patient is in waiting room. Examination room is available.
Actions	Examination room is prepared for office visit. Patient and records are moved to examination room.
Post conditions	Patient is prepared for examination. Appropriate records are moved with the patient.

Step G (a)	Nurse takes vitals.
Preconditions	Equipment for blood pressure, temperature, and other vitals are ready for use.
Actions	Nurse performs required actions for doctor examination preparation. Nurse notes collected data in patient record. Nurse notifies doctor that patient is ready for examination.
Post conditions	Patient hard-copy records are annotated and ready for doctor.

Step G (b)	Nurse takes EKG.
Preconditions	EKG equipment is ready for use.
Actions	Nurse performs required actions for doctor examination preparation. Nurse notes collected data in patient record. Nurse notifies doctor that patient is ready for examination.
Post conditions	Patient's EKG is ready for doctor.

Step H	Doctor examines patient and reviews records and EKG.
Preconditions	Patient is ready for examination. EKG results are available. Vitals information is available.
Actions	Doctor identifies potential health concerns. Doctor identifies actions to be taken to address concerns.
Post conditions	Doctor has and reviews all available information for patient.

Step I	Doctor orders additional lab work.
Preconditions	Doctor has completed review of all available information (vitals, EKG, hospital discharge, prior medical history, and other information).
Actions	Doctor completes lab order form (blood tests). Doctor updates patient records (hard copy) noting lab orders.
Post conditions	Lab order form given to patient to fulfill. Patient is released from appointment.

Step J	Hard-copy paperwork is returned to medical records unit.
Preconditions	Doctor has completed patient examination. Doctor's interaction with patient has been incorporated into patient file.
Actions	Patient file is returned to medical records area and filed.
Post conditions	Patient hard-copy medical documents are stored for future retrieval.

Step K	Office visit information is transcribed into office electronic medical record.
Preconditions	Patient hard-copy records are returned to medical records unit. Patient electronic medical record is available for update. Transcribing resource has electronic access to electronic and hard copy of medical records.
Actions	Additions to hard-copy medical record are typed into electronic patient record.
Post conditions	Electronic medical record contains all hard-copy patient data.

Step L	Patient goes to lab for prescribed tests and registers at lab desk.
Preconditions	Patient has an order for lab work. System is in place for collecting patient demographic and insurance information.
Actions	Patient insurance and billing information is collected. Doctor receives report. Medical order is entered into system.
Post conditions	Patient is queued for blood work. Medical order for lab work is properly entered into the system.

Step M	Lab paperwork prepared and queued for phlebotomist.
Preconditions	Blood specimen requirements for each requested test are appropriately characterized within the system.
Actions	Labels and orders are printed for phlebotomist.
Post conditions	Paperwork (labels) are printed for blood sample.

Step N	Phlebotomist takes blood and labels it for lab technician.
Preconditions	Printed paperwork (labels) and patient are ready.
Actions	Blood sample is taken.
Post conditions	Blood is in properly labeled vials.

Step O	Lab technician performs tests on sample and generates report.
Preconditions	Blood and paperwork are ready. Technician loads proper machine with blood sample. Bar code on vial indicates patient and proper test to machine.
Actions	Machine runs tests. Each machine sends results to lab's database collection point. Results are collated into report for transmission to the hospital repository.
Post conditions	Report exists. Blood is disposed of properly. Technician performing work is identified and linked to results.

Step P	Lab results are transmitted to hospital central repository.
Preconditions	Test results report is available in the lab repository. The lab's patient ID is matched with the hospital's patient ID. Hospital can authenticate the lab. Communications exist. Lab can authenticate hospital. Lab can provide the transmitted report to authorized readers if the request for tests came directly to them from the patient or doctor (not via the hospital).
Actions	Results are transmitted.
Post conditions	Laboratory is associated with results in hospital repository.

Step Q	Notification is given to doctor's office (email).
Preconditions	Tests are completed. Report exists. Doctor's email is provided.
Actions	Email notification that results are available is sent to doctor's office. Results are placed in patient medical record.
Post conditions	Information notification is received.

Step R	Doctor reviews test results and develops treatment plan for patient.
Preconditions	Tests are completed and report is available at hospital central repository. Doctor has received email notification. Doctor's office is able to access and retrieve report (authentication, authorization, and connectivity). Doctor has connectivity and access to electronic medical record.
Actions	Doctor reviews test report. Doctor reviews office electronic medical record.
Post conditions	Written treatment plan for patient is prepared. Plan is given to nurse to notify patient.

Step S	Treatment plan is communicated to patient.
Preconditions	Treatment plan for patient is completed. Nurse has received treatment plan from doctor. Patient contact information and mailing address is available to the nurse.
Actions	Nurse calls patient to communicate treatment plan and arrange for subsequent patient actions as required by the plan. Letter is prepared with treatment plan and information from nurse/patient discussion and mailed to patient. Treatment plan report and copy of letter are added to patient's office medical record.
Post conditions	Patient is notified (verbally and in writing) of treatment plan and future actions. Office medical record is updated with treatment plan and patient communications.

Appendix B: Reference Tables

People Reference Table

The controlling role is marked as *C*, and participants are marked as *X*.

	A1) Patient to lab	A2) Lab paperwork prepared	A3) Blood sample drawn	A4) Lab sample analyzed	A5) Report transmitted to hospital	A6) Notice sent doctor's office
Patient	X		X			
Lab check-in staff	C	C				
Phlebotomist			C			
Lab technician				C	C	

Resource Reference Table

The controlling role is marked as *C*, and participants are marked as *X*.

	A1) Patient to lab	A2) Lab paperwork prepared	A3) Blood sample drawn	A4) Lab sample analyzed	A5) Report transmitted to hospital	A6) Notice sent to doctor's office
Lab work order	X	X				
Patient insurance data	X					
HIPAA forms	X					
Lab scheduling	X	X				
Lab test repository and reporting system				X		X
Blood sample			X	X		
Lab paperwork (labels)		X	X	X		
Testing machine				X		
Testing machine connectivity				X		
Doctor office connectivity						X

Bibliography

URLs are valid as of the publication date of this document.

[Alberts 2003]
Alberts, Christopher & Dorofee, Audrey J. *Managing Information Security Risks: The OCTAVE Approach*. Addison-Wesley, 2003.

[Alberts 2005]
Alberts, Christopher & Dorofee, Audrey J. *Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments* (CMU/SEI-2005-TN-032). Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/library/abstracts/reports/05tn032.cfm

[Alberts 2008]
Alberts, Christopher; Smith II, James; & Woody, Carol. *Multi-view Decision Making (MVDM) Workshop* (CMU/SEI-2008-SR-035). Software Engineering Institute, Carnegie Mellon University, 2009. http://www.sei.cmu.edu/library/abstracts/reports/08sr035.cfm

[DOD 2009]
The Office of the Assistant Secretary of Defense for Networks and Information Integration / DoD Chief Information. *Officer Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy*. August 2009. http://cio-nii.defense.gov/docs/DoD_IA_Strategic_Plan.pdf

[Ellison 1999]
Ellison, R.J.; Linger, R.C.; Longstaff, T.; & Mead, N.R. "Survivable Network System Analysis: A Case Study." *IEEE Software 16*, 4 (July/August 1999): 70-77.

[Ellison 2007]
Ellison, R. & Woody, C. "Survivability Challenges for Systems of Systems." *News at SEI*, Software Engineering Institute, Carnegie Mellon University, June 1, 2007.

[Ellison 2008]
Ellison, Robert J.; Goodenough, John; Weinstock, Charles; & Woody, Carol. *Survivability Assurance for Systems of Systems* (CMU/SEI-2008-TR-008). Software Engineering Institute, Carnegie Mellon University, 2008. http://www.sei.cmu.edu/library/abstracts/reports/08tr008.cfm

[Howard 2006]
Howard, Michael & Lipner, Steve. *The Security Development Lifecycle SDL: A Process for Developing Demonstrably More Secure Software.* Microsoft, 2006.

[Lapham 2006]
Lapham, Mary Ann & Woody, Carol (contributor). *Sustaining Software-Intensive Systems* (CMU/SEI-06-TN-007). Software Engineering Institute, Carnegie Mellon University, 2006. http://www.sei.cmu.edu/library/abstracts/reports/06tn007.cfm

[Leveson 2004]
Leveson, N. "A Systems-Theoretic Approach to Safety in Software-Intensive Systems." *IEEE Transactions on Dependable and Secure Computing 1*, 1 (January-March 2004): 66-86.

[Maier 1996]
Maier, M. "Architecting Principles for Systems of Systems" 567-574. *Proceedings of the Sixth Annual International Symposium, International Council on Systems Engineering*. Boston, MA, 1996. www.infoed.com/Open/PAPERS/systems.htm

[Maier 1998]
Maier, Mark W. "Architecting Principles for Systems-of-Systems." *Systems Engineering 1*, 4 (Winter 1998): 267-284.

[Stamatis 2003]
Stamatis, D.H. *Failure Mode and Effect Analysis: FMEA from Theory to Execution, 2nd ed.* ASQ Quality Press, 2003.

[Woody 2005]
Woody, Carol. *Eliciting and Analyzing Quality Requirements: Management Influences on Software Quality Requirements* (CMU/SEI-05-TN-010). Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/library/abstracts/reports/05tn010.cfm

[Woody 2007]
Woody, C. & Alberts, C. "Considering Operational Security Risk during System Development." *IEEE Security & Privacy 5*, 1 (January/February 2007): 30-35.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	June 2010	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Survivability Analysis Framework	FA8721-05-C-0003

6. AUTHOR(S)

Robert J. Ellison and Carol Woody

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2010-TN-013

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	**Error! No text of specified style in document.**

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Complexity and change are pervasive in the operational environments of today's organizations. Organizational and technological components that must work together may be created, managed, and maintained by different entities around the globe. The ability of these independently developed pieces to effectively work together after they are built and integrated is uncertain and problematic. The way technology is applied by people to address an operational need must also be understood. Survivability of the organization depends on the capabilities of the people, actions, and technology that compose the operational process to work together to achieve operational effectiveness. A team of Carnegie Mellon University Software Engineering Institute (SEI) software engineers built the Survivability Analysis Framework (SAF) to examine the elements of an operational process and evaluate the survivability and effectiveness of the linkage among roles, dependencies, constraints, and risks to achieve critical operational capabilities. The SAF and the benefits achieved in its pilot use are described in this report.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Failure analysis, survivability, work process analysis, mission thread, security, operational security ,mission assurance	43

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL