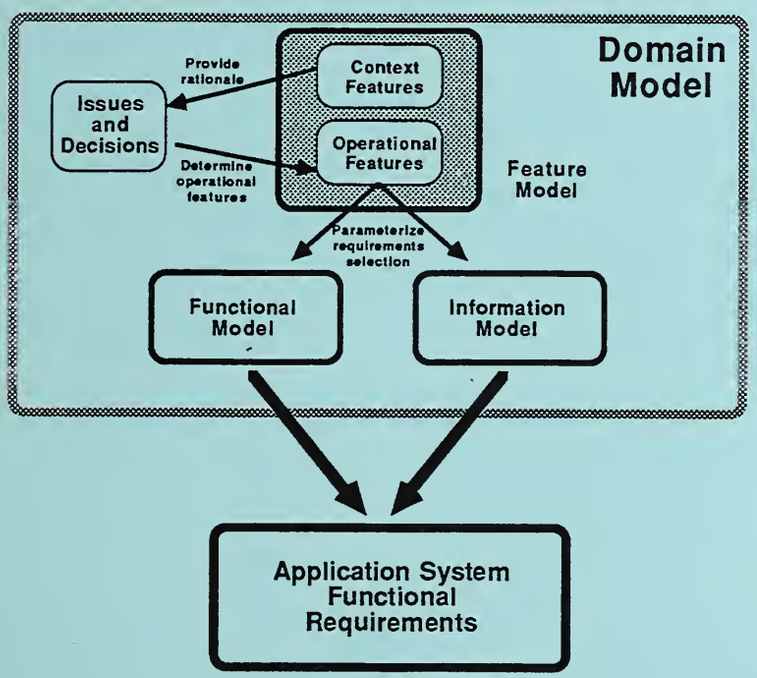
NISTIR 5494

A Domain Analysis of the Alarm Surveillance Domain

Version 1.0

Conducted as Part of the Domain Analysis Case Study Project

Christopher Dabrowski
James Watkins



U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

NIST

NISTIR 5494

A Domain Analysis of the Alarm Surveillance Domain

Version 1.0

Conducted as Part of the Domain Analysis Case Study Project

Christopher Dabrowski
James Watkins

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

September 1994

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

TECHNOLOGY ADMINISTRATION
Mary L. Good, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Arati Prabhakar, Director

ACKNOWLEDGMENTS

We would like to acknowledge the valuable contributions of GTE Government Systems Division in Chantilly, Virginia, including Richard Kramer, Richard Law, Cathy Lytle, Michael Moore, Larry Riley, John Rosner, and Linda Sveinsson. These domain experts provided most of the expertise on alarm surveillance systems that made this report possible. In particular, John Rosner was instrumental in providing information on the inner workings of surveillance systems and in identifying key components of the model described in this report. George McWilliams of the Colsa Corporation contributed valuable information on alarm surveillance systems. John Terrell, Alan Bonde, and Steve Costello of GTE Laboratories in Needham, MS reviewed parts of the domain model and suggested valuable additions.

Dr. Hasan Sayani and Dr. Cyril Svoboda of the Advanced Systems Technology Corporation (ASTEC) contributed valuable advice and review in domain engineering and semantic data modeling. Dr. Sayani supplied us with the CaMERA repository tool and assisted us with using this tool to support the domain analysis effort. Moreover, Dr. Sayani, together with his programming team at ASTEC, developed and implemented the Prototype Application Development Tool and then continued to provide support in the use of the tool during the course of the project.

We would also like to acknowledge Sholom Cohen, Patrick Donohoe, and John Leary of the Software Engineering Institute at Carnegie Mellon University for their help in the use of the Feature-Oriented Domain Analysis (FODA) Method and their review of the domain model.

Within NIST, Arnold Johnson lead the software reuse effort and reviewed the domain model. Susan Katz collaborated on the context analysis phase of this project and provided review during the early part of the domain analysis phase. Also within NIST, we would like to acknowledge the efforts of Elizabeth Fong, Margaret Law, Fran Nielson, Bob Aronoff, Mike Chernick, and others who contributed expertise or who reviewed early versions of the products of the domain analysis effort. Jeni Lindeman developed the entity-relationship diagrams in this report. Within the Ballistic Missile Defense Organization (BMDO), Greg Stottlemyer helped create the Software Producibility Manufacturing Operations Development Integration Laboratories (MODILs) and saw the need for the focus on software reuse as an area of applied research.

PREFACE

The Computer Systems Laboratory (CSL) within the National Institute of Standards and Technology (NIST) has a mission under Public Law 89-306 (Brooks Act) to promote the "economic and efficient purchase, lease, maintenance, operation, and utilization of automatic data processing equipment by federal departments and agencies." When a potentially valuable technique first appears, CSL may be involved in research and evaluation. Later on, standardization of the results of such research, in cooperation with voluntary industry standards bodies, may best serve federal interests. Finally, CSL helps federal agencies make practical use of existing standards and technology through consulting services and the development of supporting guidelines and software.

Certain commercial software products and companies are identified in this report for purposes of specific illustration. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products identified are necessarily the best available for the purpose.

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

A key to increasing software producibility in the development of large, reliable software applications is the systematic reuse of existing software products. Domain analysis is a pivotal technique for developing reusable products that can be used to engineer software systems. The Domain Analysis Case Study was created under the auspices of the Ballistic Missile Defense Organization (BMDO)[1] for the purpose of investigating domain analysis methods. This report is a product of the Domain Analysis Case Study.

1.1 The Purpose of This Report

The Domain Analysis Case Study is currently investigating the use of a particular domain analysis method. This method, called the Feature-Oriented Domain Analysis (FODA) method (described in more detail in sec. 1.5), was developed by the Software Engineering Institute at Carnegie Mellon University. The purpose of this report is to describe the results of the application of the domain modeling phase of the FODA method to the alarm surveillance domain. Domain modeling is the second phase of the FODA process. The primary product of this phase is the alarm surveillance domain model which provides a detailed description of the capabilities of alarm surveillance systems.

The results of the first phase of this domain analysis effort, in which the alarm surveillance subdomain was defined and scoped, were reported in A Context Analysis of Network Management Domain [DABR93]. An analysis of the application of both the context analysis and domain modeling phases of FODA will be described in the final report for the Domain Analysis Case Study. The final report will recommend the characteristics a domain analysis method should have in order to be used in real-world software development.

1.2 The Alarm Surveillance Domain

Domain modeling is the heart of the domain analysis process. A domain can be defined as a class of systems that have similar requirements and capabilities. In this report, the domain of interest is alarm surveillance; the class of systems is alarm surveillance software systems. Alarm surveillance is a subdomain of the network management domain. Network management systems are software systems that monitor and control communications networks to ensure their continuous operation, efficiency, and integrity. Alarm surveillance systems monitor communications networks to detect and report information about faults.

---

[1]The BMDO was formerly known as the Strategic Defense Initiative Organization (SDIO).

The objective of domain modeling is to create a model of the capabilities of systems in the alarm surveillance domain. In the domain model, information used in developing alarm surveillance systems is identified, captured, and organized so that it can be reused to engineer new alarm surveillance systems. The domain model documents commonalities that characterize the functions and data structures of systems in the domain as well as differences that are specific to subsets of systems in the domain. The FODA method provides a mechanism--called features--that are organized into a feature model or catalogue. Features allow the model to be adapted or specialized to produce functional requirements for new systems in the domain. During the development of alarm surveillance application systems, the feature model can be used to guide the adaptation of the domain model to produce specifications for new alarm surveillance systems.

1.3 The Audience for This Report

The audience for this report includes, but is not limited to:

- Government personnel and contractors who are interested in domain analysis methods and are, in particular, interested in applying the FODA method.
- Experts in network management and developers of network management systems within government and industry who may wish to use the products of the Case Study.
- Information systems developers who intend to develop domain models for other domains who want an example of a domain model.
- Purveyors of domain analysis methods who wish to gain further understanding of the application of domain analysis methods.

This report will be available to all interested parties. Comments and cooperative follow-on research efforts are welcome.

1.4 The Domain Analysis Case Study

The purpose of the Domain Analysis Case Study is to examine the potential use of domain analysis methods. The specific goals of the Case Study are to:

(1) Test the viability of domain analysis as a process to aid software reuse.

(2) Identify the processes and products necessary to meet the goals of domain analysis in developing reusable components.

(3) Identify the characteristics that determine a method's usability; i.e., evaluate the ease with which developers may use the method to create the products of domain analysis.

(4) Identify requirements for domain analysis support tools.

The strategy of the Case Study is based on direct "hands on" experience in the use of the method on a practical problem. During the Case Study, key aspects of the use of the method have been documented. This has included documenting the use of selected FODA procedures to develop domain analysis products. It has also included documenting the use of domain analysis products to engineer applications within the domain.

1.5 The FODA Process

The FODA method and its current applications are described in [KANG90], [PETE91], and [COHEN92]. At present, the FODA method consists of three phases: context analysis phase, described in [DABR93]; the domain modeling phase; and the architecture modeling phase. These phases will be briefly described below to provide the reader with necessary perspective. A detailed description of the products of the context analysis and domain modeling phases will be deferred until sections 2 and 3.

1.5.1 Context Analysis

The context analysis phase establishes the scope and boundary of a domain of interest. The context analysis specifies what major functions and capabilities are within the domain and what functions and capabilities are outside the domain. In the FODA approach, context describes the circumstances, situation, or environment in which a particular domain exists. The context analysis identifies important elements that are external to the domain. It defines the relationships and interactions that exist between the domain and these external elements.

An important part of the context analysis is to describe how the function and behavior of external entities may vary. The context analysis establishes how this variation (1) affects interactions between the domain and its external elements and (2) in a broad sense, influences requirements for systems within a domain. Understanding variation in context provides a basis for detailed analysis of variability among systems in the domain during the subsequent domain modeling phase.

The FODA method also recommends making an assessment of the potential for developing reusable software within the domain. This assessment is intended to describe the feasibility of developing reusable components within the domain together with the economic payoff that would result from doing so. The report: A Context Analysis of the Network Management Domain describes the results of the application of the first phase of the FODA method--the context analysis phase--to the network management domain.

1.5.2 The Domain Modeling Phase

The domain modeling phase is directed toward describing the capabilities of, and requirements for, systems within a domain of interest whose scope was defined in the context analysis phase. The principal product of this phase is a domain model. The domain model consists of three components:

- The Feature Model represents the end user's view of the capabilities of systems in the domain. Features describe visible aspects of systems that directly affect end users. The Feature Model contains features that are mandatory for all systems in the domain as well as features that are optional or that represent alternative choices. The Feature Model is used by application developers to define capabilities that their applications should have. An analysis of tradeoffs in selecting particular optional and alternative features is documented in the descriptions of *Issues and Decisions*. Issue/Decision descriptions guide application developers in selecting features. In the FODA approach, the selection of optional and alternative features in the Feature Model parameterizes the Functional Model, described below. This parameterization results in the adaptation of the domain model to produce requirements for individual application systems in the domain.

- The Functional Model describes the functions, data flows, and control flows of systems *within the domain of interest* (This is in contrast with the data flows *between the domain of interest and external entities in the context model*, described in sec. 2.2.1). The FODA Functional Model is based on the well-known conventional systems analysis techniques for representing data transformations and state transitions. The Functional Model extends these modeling techniques to identify those capabilities and requirements that are common among the systems and to describe how particular functions may be specialized for individual systems within the domain. In the FODA approach, this specialization is parameterized by selection of features, as described above.

- The Information Model describes the major domain entities, their internal structure, and relationships between entities in the domain of interest. The Information Model represents the essential domain knowledge that is necessary to create other reusable components. In the FODA approach, this model is used to ensure that the proper data abstractions are used to develop Information Models for application systems within the domain. In the domain model for alarm surveillance, the specialization of the Information Model is also parameterized by the selection of features.

Figure 1.1 describes graphically the relationship between the three domain model components.

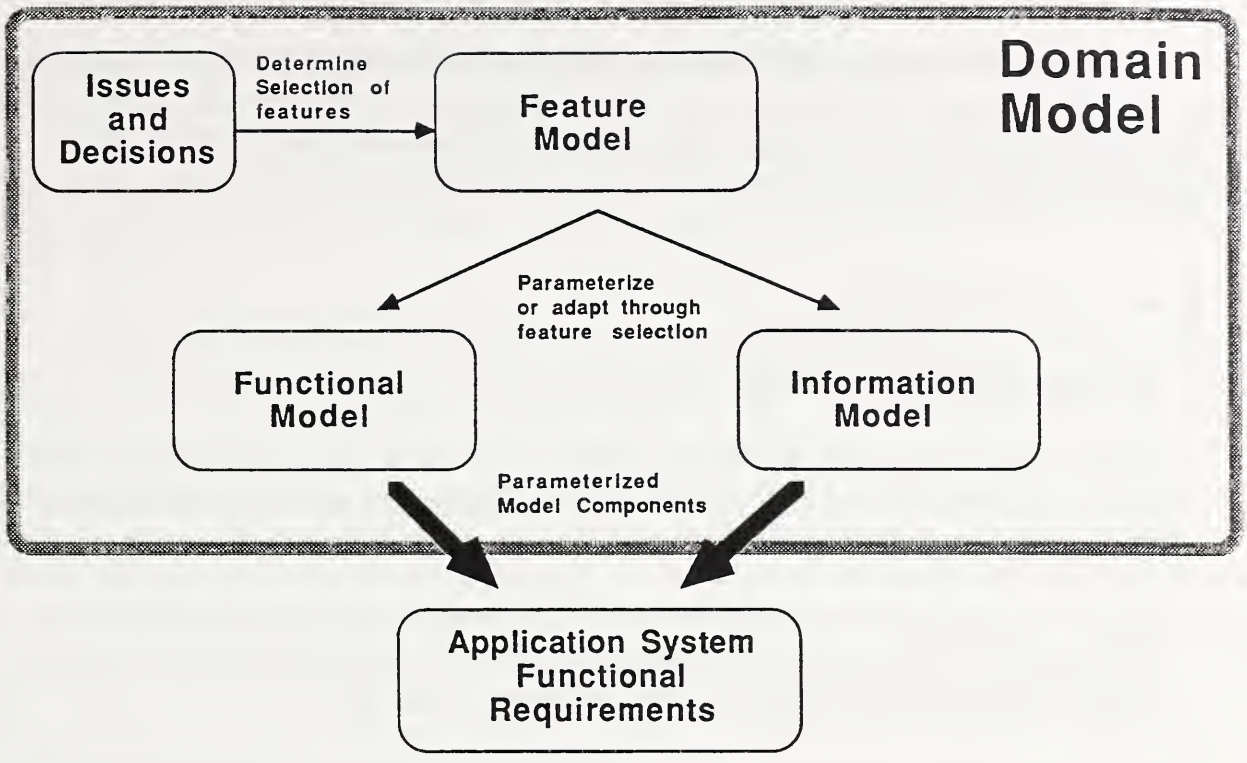


Figure 1.1: The Relationship Among Domain Model Components

The generation of application system functional requirements is shown at the bottom of the diagram.

The domain model may be distinguished from an analytical model produced by traditional systems analysis techniques in two respects. First, the Functional and Information Models produced are extended to represent commonalities and variabilities for a class of systems. Second, a Feature Model is developed for the purpose of adapting the Functional and Information Models to produce application systems within the domain. Traditional systems analysis techniques produce a model that is valid only for the application under development. The elaboration of these distinctions is one of the tasks of this report.

1.5.3 Architecture Modeling

During the architecture modeling phase, a domain architecture is developed. The domain architecture describes a high-level design or "blueprint" for implementing software applications in a domain. The domain architecture is also a reusable component. The entire architecture, or selected parts of it, can be adapted to develop designs for specific applications within a domain. To accomplish this, the domain architecture may contain information on how the requirements described in the domain model are to be implemented as software systems. The domain architecture describes how requirements in the domain model are mapped to specific design components within the architecture. Use of a domain architecture eliminates the need for having to develop designs for individual software applications from scratch.

The FODA method prescribes the beginning architectural modeling to be initiated during domain modeling [COHEN92]. However, at present, the Case Study is scheduled to end after the domain modeling phase. Therefore, this report will not describe the development of the domain architecture.

1.6 How to Read This Report

The organization of the report is as follows:

- Section 2 provides a review of the context model for the network management domain, described more fully in the report A Context Analysis of the Network Management Domain [DABR93].

- Section 3 provides an overview of the domain model for alarm surveillance, describing at a high level of detail the three major subcomponents: the Feature Model, the Functional Model, and the Information Model.

- Section 4 provides a detailed description of the Feature Model for the alarm surveillance domain.

- Section 5 provides a detailed description of the Functional Model for the alarm surveillance domain.

- Section 6 provides a detailed description of the Information Model for the alarm surveillance domain.

- Section 7 contains the references.

- Appendix A contains the expanded domain dictionary, begun during the context analysis phase. Appendix B contains (1) correspondences between the data and control flows in the Functional Model and particular structures in the Information Model, (2) correspondences between particular functions in the Functional Model and information structures they use, and (3) type hierarchies used in both the Functional and Information Models. Appendix C provides supplementary decomposition for the Functional Model.

2. REVIEW OF THE PRODUCTS OF THE CONTEXT ANALYSIS

In this section, the context model is reviewed. The context model was produced in the preceding context analysis phase [DABR93]. The context model established the context, or environment, for alarm surveillance systems and provided the basis for developing the domain model.

The communications networks and the network administrator form the most important elements of the context of alarm surveillance domain. The communications network consists of the physical network, including the transmission medium and the devices, together with the communications services that enable transmission of information to take place. The network administrator is the person responsible for ensuring that the network is managed in a satisfactory way. The capabilities of an alarm surveillance system are directed toward satisfying needs of the network administrator for monitoring and analyzing information about the status of a communications network. Alarm surveillance systems are the principal tool by which the network administrator learns the status of the communications network. In the FODA approach, the domain model must take into consideration the characteristics of communications networks, the network administrator, and the other external entities with which alarm surveillance systems interact.

Three principal products of the context analysis are most important to review: the definition statement of alarm surveillance, the context diagram, and the description of variability in the context. The definition statement provides a narrative description of alarm surveillance functions. The context diagram shows the data and control flows between the alarm surveillance domain and its external entities. Together with the definition statement for the alarm surveillance domain, the context diagram defines the boundary of the domain. Identification of variability in the context provides a foundation for understanding commonalities and differences in the domain model. The assessment of feasibility for developing products in the alarm surveillance domain, mentioned in section 1.5.1, is discussed more fully in section 6 of the report A Context Analysis of the Network Management Domain [DABR93]. A dictionary of terms defined during the context analysis that are used in this report is listed in Appendix A.

2.1 Definition of Alarm Surveillance

Alarm surveillance is concerned with the monitoring of a communications network and the management of information describing its status. The capabilities of an alarm surveillance system can be more completely defined as follows:

(1) Monitoring the network to gather information on faults and fault-related conditions.

(2) Analysis of information about faults to identify those alarm notifications describing faults that are affecting, or most likely to affect, the operation of the network.

(3) The control of the dissemination of information about faults to prevent transmission of redundant or irrelevant information and to ensure that (a) the resources of the communications network are directed only toward the most critical faults and (b) genuine reports are sent to appropriate destinations.

Alarm surveillance excludes the diagnosis of faults and the correction of problems caused by faults. It also excludes tracking of the progress of resolving faults. In [DABR93], these activities are described as domains that are distinct from alarm surveillance and that, like alarm surveillance, are part of the higher-level domain of network management.

2.2 The Context Diagram for Alarm Surveillance

The context diagram for alarm surveillance is presented below. This diagram is an updated version of the context diagram presented in [DABR93]. The updates reflect changes in the understanding of the boundary of the domain that occurred during the domain modeling phase.[2]

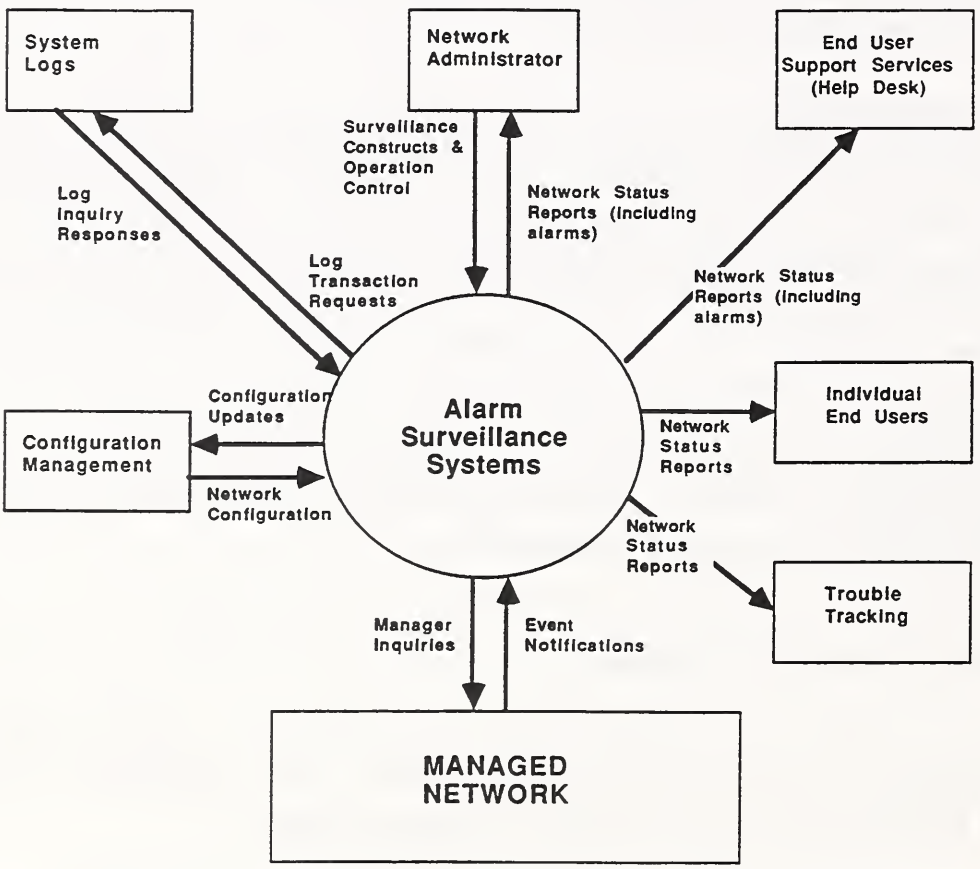


Figure 2.1: The Context Diagram for Alarm Surveillance

[2]This issue is addressed more fully in the Domain Analysis Case Study final report.

2.2.1 Explanation of Data Flows

To match the external entities in the context diagram to the entity descriptions in the previous section, the reader should start with the Network Administrator entity and proceed in a clockwise direction.

- **The Network Administrator**

  These persons receive information on the status of the network from the alarm surveillance system, including reported alarms. Network administrators control how surveillance functions, including monitoring, filtering, and analysis, are performed. They also supply filtering and analysis constructs that determine how the alarm surveillance system performs these functions. Network administrators initiate changes in the operation of the network in response to significant changes in the network's state or changes in the way the network is being used. These interactions are carried out by means of an operator interface with graphics user interface capabilities.

- **End User Support Services (Help Desk)**

  A help desk located at a network operations center may receive network status reports, including reported alarms, from the alarm surveillance system.

- **Individual End Users**

  Under some circumstances, the network management system provides selected reports on the state of the network, including alarms, directly to the end users.

- **Trouble Tracking**

  Trouble tracking, a subdomain of fault management outside of alarm surveillance, is described in section 5.1.1 of A Context Analysis of the Network Management Domain [DABR93]. The alarm surveillance system reports event notifications, including alarms, and other network status information to a trouble tracking system.

- **The Managed Network**

  The alarm surveillance system sends inquiries on state of network resources to individual agent systems within the managed network and receives responses. The data flows between manager and the agent depict:

  (1) Manager inquiries sent from a manager to agent.

  (2) Event notification, including responses to manager inquiries, that are sent from agents to managers.

- **Configuration Management**

  Configuration management, a subdomain of network management outside the scope of alarm surveillance, is described in section 3.1.3 of [DABR93]. The alarm surveillance system receives network configuration data from configuration management. The use of this information will be described in detail in sections 5 and 6 of this report. The alarm surveillance system also updates the configuration database to reflect the affects of faults on the operation of network resources.

- **System Logs**

  The alarm surveillance system sends log transaction requests to the system log. Event notifications are recorded in the system log. To correlate events, the alarm surveillance system retrieves previously logged information about faults.

It should be noted that this context diagram differs from that found in [DABR93]. The differences in the diagram reflect improvements in the understanding of the domain's context that were obtained during domain modeling. The most important changes involve the removal of System Logs from inside the alarm surveillance domain to the domain's context. The justification for this change is that System Logs are separate entities that store information used by many functions of network management besides alarm surveillance. They were therefore factored out of the alarm surveillance domain. Individual end users were added as an external entity since it was discovered that reported alarms in some cases can be sent directly to end users. The Performance Management external entity, present in the context diagram in [DABR93], was removed. During domain analysis, it was found that Performance Management data was not used extensively by alarm surveillance systems.

2.2.2 Further Definition of Domain Scope

In this report, the scope of the domain was further restricted in two ways:

(1) The domain is restricted to manager software systems; i.e., systems that initiate monitoring activity and perform analysis functions. Agent systems, that reside on network devices and other network resources, are considered outside the domain.

(2) The scope of the domain is focussed on individual alarm surveillance systems, rather than groups of such systems. Alarm surveillance systems that monitor different portions of the managed network are treated as external entities. The set of alarm surveillance systems that serve an entire communications network are organized into a network management architecture. This architecture is placed outside the scope of the domain. Communication between a particular alarm surveillance system and other manager systems is considered to be an interaction between an alarm surveillance system and its context, as is communications with the managed network itself.

2.3 Variability in the Context

Variability in the context of alarm surveillance systems was discussed in detail in section 5.4 of the report A Context Analysis of the Network Management Domain [DABR93]. This variability impacts variability in data flows across domain boundaries and variability in requirements for systems in the domain. Thus, variability in context forms the basis for capturing information about differences among systems in the domain model.

Variabilities in characteristics of communications networks were the most important aspect of variability of the alarm surveillance context. Communications network variabilities were organized into four areas:

(1) Physical variations in the structure of the communications network including its size, scope, and topology.

(2) Variability in network resources to be managed.

(3) Variability in operational requirements of the communications networks, including different operating modes the network may be in at any time.

(4) Variability in the administrative and political divisions of the managed network.

During the domain modeling phase, the description of variability in the context forms a basis for identification of context features. Context features are described in section 3.2.2.1 and in section 4.2 of this report.

3. OVERVIEW OF THE ALARM SURVEILLANCE DOMAIN MODEL

This section provides an overview of the FODA domain model of alarm surveillance and outlines the structure by which the reader may understand the domain model described in the rest of this report. First, the purpose of the domain model is explicitly stated. Then the major parts of the domain model, introduced in section 1.5 of this report are described. These parts, termed *submodels*, include: the Feature Model, the Functional Model, and the Information Model. These are represented graphically in figure 3.1.

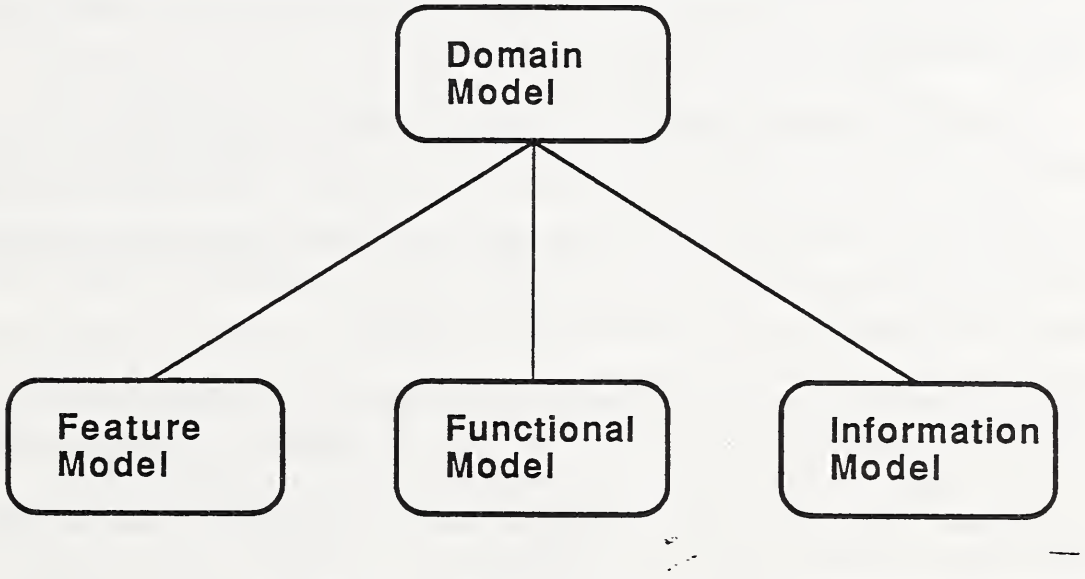


Figure 3.1: The FODA Domain Model

The relationships between the submodel are identified, and the role of each submodel in application systems development is described.

3.1 The Objective of the Domain Model

The domain model identifies and organizes the description of capabilities of systems in the alarm surveillance domain. This description includes capabilities that are common to all systems in the domain and capabilities that vary among systems. The objective of the domain model is to serve as a reusable product that can be used by developers of alarm surveillance systems to derive requirements specifications for new systems or to ensure that previously developed requirements specifications are complete. The developers would be systems analysts, experienced in the development of network management applications.

In keeping with current government and commercial practices, the functional requirements derived from the domain model would be used to support procurement of network management COTS products as well as for software development. The Military

Standard DoD-STD-2167a [DoD88] is an accepted guide to the specification of defense system software products. If the domain model should be used for DoD-related production purposes, the Prototype Application Development Tool, described in section 3.6, could be adapted to produce products that are compatible with DoD-STD-2167a.

3.2 Feature Model Overview

Features are visible aspects of systems that directly affect end users.

3.2.1 Model Objectives

The objective of feature analysis is to develop a model of the end user's understanding of the general capabilities of application systems in the domain. In the alarm surveillance domain, the end user is the network administrator. In the alarm surveillance feature model, features describe how the network administrator may define and control (1) the way the communications network is monitored and (2) the filtering, analysis and distribution of the information obtained through monitoring.

The Feature Model is the chief means of communication between network administrators and application developers. The alarm surveillance features are meaningful to network administrators and can assist the requirements analyst in deriving system specifications that will provide desired alarm surveillance capabilities. In the alarm surveillance feature model, features are organized into a catalogue form in which selection of individual features can be used to parameterize other parts of the domain model to produce functional requirements for individual alarm surveillance systems.

3.2.2 Feature Model Components

The Feature Model organizes the features of a domain to present a coherent view of the capabilities of the domain's systems. The Feature Model has three subcomponents.

3.2.2.1 Context Features

According to FODA, context features describe characteristics of the context of the domain as seen by end users. The development of context features is based on the analysis of variability in the context of the domain, described above in section 2.3. In the alarm surveillance domain, context features focus on the characteristics of communications networks that are most relevant for alarm surveillance from the point of view of the network administrator. Both common and variable context features are described. The selection of specific variable context features serves to define the context of a particular alarm surveillance system (as will be described in more detail in sec. 3.2). Five groups of context features are described for the alarm surveillance domain:

- **Management Architecture**

  These features describe the type of network management architecture for the communications network being monitored and the position of the alarm surveillance system within that architecture.

- **Global Network Structural Characteristics**

  These features define quantitative factors that describe the global structural characteristics of the network that will affect how the network should be monitored. This includes the network size (number of devices and other managed network resources), number of subnetworks to be monitored, network topology, and bandwidths. The entity relationship model describes specific structures for representing this information.

- **Individual Network Resource Characteristics**

  These features describe the aggregate characteristics of individual network resources (both network devices, other resources, and agents) that, in part, determine how they should be monitored. The entity relationship model describes specific structures for representing this information.

- **Communications Network Operating Modes**

  These features define operating modes that a communications network may assume. Operating modes are states a network may be in, such as peacetime or wartime. (Four categories of operating modes have been defined.) The existence of operating modes and the necessity to change modes affects the selection of operational features.

- **Staffing Requirements**

  These features describe requirements for staffing a network management station.

Context features are described in detail in section 4.2 of this report. The context features represent further definition of the variability in the context of network management described in section 5.4 of A Context Analysis of the Network Management Domain [DABR93].

3.2.2.2 Operational Features

These features describe the functional characteristics of alarm surveillance systems. Operational features describe the services the system must provide to the network administrator. Operational features also describe the means available for the administrator to define and control alarm surveillance activity. These features are grouped as follows:

- **Monitoring**

  Monitoring features allow the network administrator to define the part of the network that will be monitored, to organize network resources into different groups for monitoring purposes, and to determine the method by which information is gathered.

- **Filtering**

  Filtering features allow the network administrator to control the dissemination of event notifications reporting information on faults and to screen out redundant or irrelevant notifications.

- **Analysis**

  Analysis features allow the definition and control of functions that interpret and correlate event notifications to identify alarms describing genuine faults that are most likely to affect the network.

- **Network Management Protocols**

  These features specify what standard network management protocols the alarm surveillance system will respond to. (Though management protocols are actually outside the scope of alarm surveillance, they have been included to better understand the application of domain analysis to modeling system interfaces.)

- **Dynamic Control**

  These features allow the network administrator to program and control automatic, coordinated changes in monitoring, filtering, and analysis activity to meet changes in the communications network environment. These features satisfy requirements for responding to planned or unplanned contingency situations, to support military survivability strategies and planning, and to implement "lights out" policies.

Operational features are described in greater detail in section 4.3 of this report.

3.2.2.3 Representational Features

These features define the characteristics of user interfaces of systems in the domain. Since alarm surveillance systems are software systems that do not directly interact with network administrators, this part of the Feature Model was not developed.

3.2.3 Feature Model Structure

The three components of the Feature Model are organized in a structure in which more general features are found at higher levels and more specific features at lower levels. The more general features form the basis for more specific features that describe capabilities in greater detail. Within the Feature Model hierarchy, there are three types of features:

- Mandatory Features are common to all systems in the domain.
- Alternative Features are organized in sets of features in which individual alternatives represent mutually exclusive choices for individual systems in the domain.
- Optional Features are features that individual systems may or may not have.

Mandatory features represent commonality in the domain--features that all systems in the domain have. Alternative and optional features identify areas of variability--features that subsets of systems may have. During application systems development, the Feature Model is examined to select alternative and optional features appropriate for the system being developed. The automatic selection of mandatory features together with the selection of optional and alternative features define the (1) the characteristics of the context of a particular alarm surveillance system and (2) the operational capabilities of the application system to be developed. The relationship between the selection of context and operational features will be described in the next subsection.

The Feature Model may contain specific rules that define additional relationships between features. These rules affect the selection of features. Two such rules involve constraints and dependencies. Constraints specify that the selection of one feature precludes the selection of another. Dependencies specify that the selection of one feature requires the selection of another.

Figure 3.2 shows the features in the part of the operational feature hierarchy that allows the network administrator to define the scope of the network to be monitored.

4.3.1.1 Monitoring Scope Definition and Control
a) Select Alternative Monitoring Organization
a.1) **Consolidated (Alternative)**
a.2) **Partitioned (Alternative)**
a.2.1) **Define Network Partition**
a.2.2) **Enable/Disable Network Partition**

Figure 3.2: An Example Feature Hierarchy

The highlighted features allow the selection of alternative monitoring organizations. The selection of consolidated monitoring organization means that all resources in the managed

network will be monitored together. The selection of partitioned monitoring organization means that the resources can be divided into subsets that can each be monitored in a different way. In this segment, note that the selection of either alternative constrains the selection of the other. This portion of the operational feature hierarchy is elaborated in section 4.3.

3.2.4 Model Interrelationships

Context features, overviewed in section 3.2.2.1, are derived from the description of variability in the context. During the context analysis phase, areas of variability are identified and described. During feature analysis, these areas of variability are refined, sharpened, and focused into descriptions of specific features. The notion of variability is formally refined into sets of optional and alternative features.

During requirements analysis, the context features are carefully examined to identify elements that describe the context of the application system being developed. The selection of alternative and optional context features constitutes a definition of the context of the application system. For the communications network, this selection defines the size and topological characteristics of the network to be monitored, the characteristics of devices and other network resources to be managed, the modes of operation the network will assume, and its staffing requirements.

The selection of context features serves as a guide for selecting alternative and optional operational features that the application system will need. The selection of operational features provides the application system with capabilities that will be needed to monitor the communications network defined by the selection of context features, to filter and analyze event notifications, and to perform other functions necessary for alarm surveillance. To assist in making these selections, each optional and alternative operational feature is accompanied by an Issue/Decision description.

3.2.5 Issues and Decisions

Within the domain model, *issues* are associated with the selection of optional and alternative operational features that should be made in order to produce functional requirements for individual alarm surveillance applications systems. *Decisions* describe alternative choices or resolutions that can take place. The application developer uses issues/decision descriptions as a guide to the selection of features.

In the application of the FODA method to the alarm surveillance domain, an issue is accompanied by a detailed description of the selection to be made. In this description, the specific operational feature for which the issue is raised is identified. Alternative decisions are identified and accompanied by justifications--known as rationales--for the choice. Rationales are based on the selection of particular optional and alternative context features that define the context of an alarm surveillance system being developed.

The selection of operational features using Issue/Decision descriptions parameterizes both the Functional Model and Information Model to produce functional requirements for specific systems in the domain. Figure 3.3 refines figure 1.1 to show the relationship between context features, operational features and Issue/Decision descriptions. The figure shows the parameterization of the Functional and Information Models to yield application system requirements.

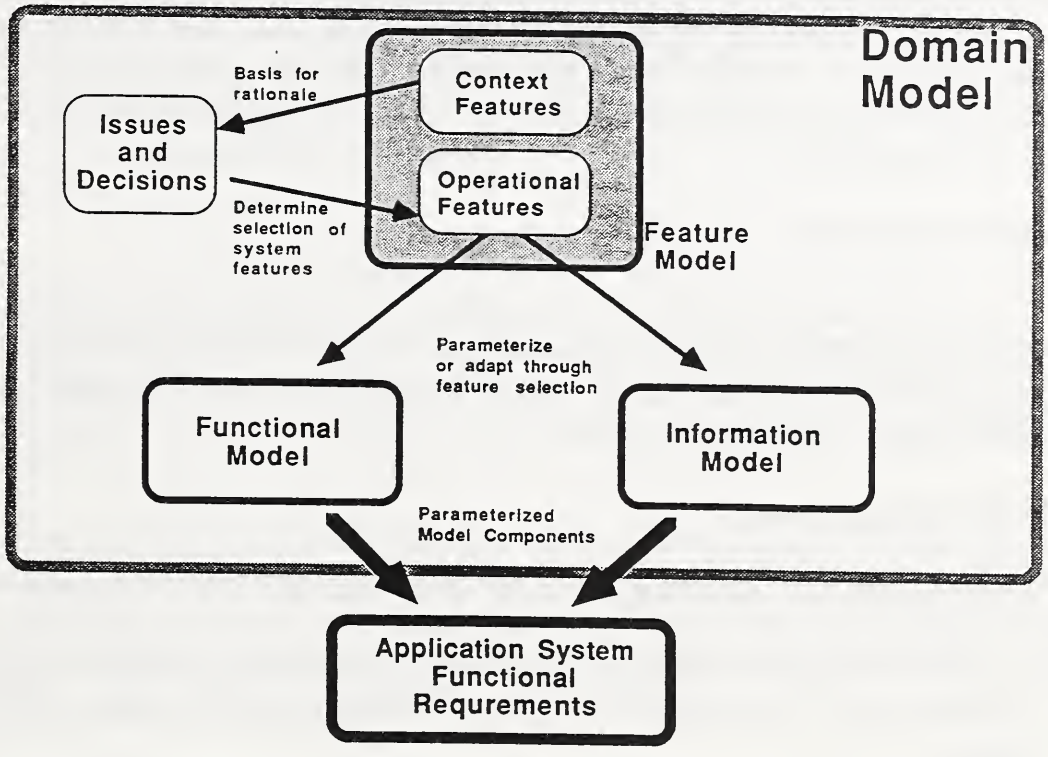


Figure 3.3: Relationship Between Components of the Feature Model

The parameterization of the Functional and Information Models is described further in section 3.3 and section 3.4.

The selection of features and the parameterization of the models are complex processes. Context features for the domain must be weighed carefully, and where appropriate, quantitative formulas should be used to make decisions. Dependencies and constraints existing between features also must be taken into account. The complexity of the feature selection process calls for automated tool support. The prototype Application Development Tool, described in the section 3.6, was created to provide this support.

3.3 Functional Model Overview

Functional analysis identifies the commonalities and differences in the function, data flows, and control flows of systems in the alarm surveillance domain. This analysis is intended to describe the functions that software systems are to perform in order to provide the operational features discussed in section 3.2.2.2. Functional analysis abstracts and then structures the common functions found in the domain and the sequencing of those actions into a model. The Functional Model, described in detail in section 5 of this report, defines data transformations performed by functions, identifies controls, and describes the sequence of actions that take place. The data structures used by particular functions in the Functional Model are described in the Information Model. Cross references between the two models are described in Appendix B.

3.3.1 Model Objectives

The Functional Model provides the application developer with a detailed description of the behavior of software systems in the domain. Using the Feature Model, the Functional Model can be parameterized to provide application developers with functional requirements for individual alarm surveillance systems.

3.3.2 Model Components

In this section the major components of the Functional Model are described:

- o An overview of the functional decomposition of alarm surveillance together with the correspondence of particular functions to the features in the Feature Model they support.
- o The descriptions of data transformations and controls associated with particular functions--necessary to describe what particular functions do.
- o The State Transitions that describe the procedures for each function.

Each of these components is described in more detail in section 5 of this report.

3.3.2.1 The Functional Decomposition

Figure 3.4 provides an overview of the decomposition of functions in the domain. This overview only shows the structure of the decomposition which is more fully described in section 3.3.2.2 and section 5 of this report. Beginning with the representation of the alarm surveillance function provided in the context diagram, the decomposition of more general functions into more specific functions is described in detail. The decomposition in figure 3.4 uses as its starting point the alarm surveillance function itself, defined in the context diagram in section 2.

A0 Alarm Surveillance: Manager Function (Context Level)
- A1 Process Incoming Transmissions
- A2 Perform Surveillance Functions
  - A21 Control Surveillance Constructs
  - A22 Enforce Scope of Responsibility
  - A23 Analyze Events
    - A231 Filter Events
    - A232 Analyze Poll Responses
    - A233 Correlate Events
    - A234 Determine Alarm Disposition
    - A235 Identify Alarm Destinations
  - A24 Compute Summary Report
- A3 Poll Agents
- A4 Process Outgoing Messages

Figure 3.4: Decomposition Overview

A1 performs the essential function of translating incoming messages from an agent system into an understandable, internal representation. A4 performs the reciprocal function for outgoing messages. A1 and A4 describe software functions associated with **Management Protocols** feature.

A2 performs the most important functions of alarm surveillance. Within A2, A23 performs the core functions associated with analyzing incoming notifications to identify notifications describing faults that need to be reported. A23 describes the detailed functions that software is to perform in order to provide the **Filtering** and **Analysis** features described in section 3.2.2.2. These functions include:

- o Filtering notifications to eliminate irrelevant or redundant information.
- o Analyzing responses to polls to identify resources that are non-responding and may therefore be experiencing faults.
- o Correlating notifications to identify more general problems within the network.
- o Determining whether notifications that have been filtered and correlated should be reported or whether a different action should be taken.
- o Identifying destinations to which reported alarms should be sent.

A21 is concerned with the automated capabilities for controlling the operations of filtering, analysis and monitoring constructs needed to provide the **Dynamic Surveillance Control** feature. A22 performs the essential function of ensuring that the messages processed by an alarm surveillance system falls within the purview of responsibility of that system. This function is specified to provide the capabilities described in the **Monitoring** feature. A24 is an optional summarization function that provides a measure of the overall status of a network being monitored. A3 describes the specific functions of polling the communications network that must be specified to provide aspects of the **Monitoring** feature.

The descriptions of individual functions are elaborated in the next model component: the data transformation and control component.

3.3.2.2 Data Transformation and Controls

In this model component, the individual functions identified in the functional decomposition overview are augmented with detailed descriptions of the actions they perform, their input and output data flows, and the controls that may be applied to these functions. Input flows, output data flows, and detailed descriptions indicate what data transformations the function carries out. Control flows indicate the constraints on the actions taken by the function that are exercised by external sources or by other functions. This information is represented diagrammatically, as a set of IDEF0 diagrams which follow the decomposition overview.[3] The procedure by which the function carries out its actions is described by State Transition diagrams--overviewed in following section.

In the alarm surveillance domain model, the functional decomposition and data transformation descriptions extend traditional IDEF0 modeling to identify commonalities and variabilities within the Functional Model for the domain. These IDEF0 diagrams for the domain model identify specific functions, data flows, and controls that are common to all systems in the domain. For some common functions, the diagrams identify specializations that represent capabilities needed by systems under particular circumstances; these specializations represent variabilities among systems in the domain. Data flows and controls are also identified that not specializations of common functions, but that are instead optional functions that are specific to systems with particular requirements. Such optional data flows and controls also represent variabilities among systems in the domain.

3.3.2.3 State Transitions

State transition descriptions specify the procedure by which individual functions in the Functional Model carry out data transformations. State transition descriptions define:

(1) The sequence of actions performed by an individual functions.

(2) The states that a particular function may enter into as a result of specific actions.

The model for state transitions used is based on a basic Finite State Machine Model, described in more detail in section 5.

State transition information may be used by the application developer to define specific requirements for system behavior. In the alarm surveillance domain model, state

---

[3]Please note that IDEF was selected for this domain and is not required by FODA.

transition diagrams are provided only for the lowest level of decomposition. State transitions are described for both common and variable functions.

3.3.3 Parameterization of the Functional Model

As indicated in section 3.2, in the FODA method the selection of features is said to parameterize the Functional Model for the domain. In this domain model, parameterization means that the selection of specific alternative and optional operational features determines the form the Functional Model will take for a specific alarm surveillance system. In the alarm surveillance domain model, parameterization may consist of:

- Selection of particular functions, data flows, controls, and state transitions needed to provide the capabilities called for by the feature.

- Determining how a more generic function, data flow, controls, or state transitions are specialized into more defined forms to provide needed capabilities called for by the feature.

The Functional Model is also related to the Information Model. The Information Model provides a basis for the abstract data structures that are needed to support functions described in the Functional Model. Appendix B describes the specific links that exist between individual functions and the information structures that these functions use. These links are of two kinds: (1) correspondences between data and control flows and the information structures that describe these flows in more detail (provided in Appendix B.1) and (2) correspondences between functions and the information structures that they either create, read, update, or delete (provided in Appendix B.2).

3.4 Information Model Overview

The Information Model for alarm surveillance is described in detail in section 6.

3.4.1 Model Objectives

In the FODA approach, information modeling captures and defines the domain knowledge and data requirements that are essential for implementing application systems in the domain. In the alarm surveillance domain, domain knowledge includes information structures describing network resources and their interrelationships, the reports that describe events occurring on network resources and the operating status of those resources, and the structures needed to analyze and filter events. Application developers need this information in order to understand the problems alarm surveillance systems address.

According to FODA, the Information Model is used primarily during requirements analysis to ensure that the proper data abstractions and decompositions are used during the

development of an alarm surveillance application system. The Alarm Surveillance Information Model describes the specific information structures that will be used by functions in the Functional Model. Specific linkages between the Functional and Information Model are described in Appendix B.

In the Alarm Surveillance Information Model, both common and variable information structures, including entities and relationships, are represented. Most information structures represent commonalities within the domain. Entities and relationships are also identified that are specific to subsets of application systems in the domain. The inclusion of these variable structures in the functional requirements of application systems is parameterized by the selection of optional and alternative features. These parameterizations are identified in the detailed descriptions of individual information structures, provided in section 6 of this report.

3.4.2 Model Content

Section 6 of this report first provides a high-level overview of the Alarm Surveillance Information Model. This is followed by detailed description of three major categories of information structure:

- **Information Structures That Support Network Management Communications**

  This category of information structures consists of entities and relationships that define types of transmissions between managers, agents, and other communicating entities. These transmissions exchange messages relating to the detection and reporting of potential faults. Together these information structures describe the data that is exchanged in order to perform alarm surveillance. These information structures support the function A2 **Analyze Events** by providing a description of the data structures to be filtered, correlated, and reported. The information structure descriptions are also used to support the **Process Incoming Transmissions** and **Process Outgoing Transmissions** functions.

- **Information Structures That Support Intelligent Surveillance**

  This category consists of the entities and relationships that are necessary to describe (1) event profiles for filtering and (2) analysis rules for performing analysis functions. Also included are data structures for organizing resources to be monitored. Several types of data structures that represent variability in the domain are also described, including construct sets for organizing event profiles and analysis rules. Variable structures also include network partitions that allow managed resources to be placed into subsets that can be monitored separately. All of these information structures are used to support the monitoring and analysis functions within **Analyze Events** and to organize the monitoring of resources in **Enforce Scope of Responsibility** and **Poll Agents**. Their operation is controlled by the function **Control Surveillance Constructs**.

o **Information Structures That Represent the Network Configuration**

This category consists of entities that represent particular types of network resources in the managed network. The descriptions focus on the characteristics of devices and other network resources that are relevant to alarm surveillance. Containment and connection relationships between network devices are defined. Together these entities and relationships describe those parts of the network configuration that are needed to perform alarm surveillance. Specifically, these information structures support the **Enforce Scope of Responsibility** function by describing the resources to be monitored. They support the correlation function within **Analyze Events** by describing relationships between resources. They also support the **Poll Agents** function by describing the resources to be polled.

3.5 Process Overview and Highlights

The FODA process description provides general guidelines for developing domain model products, but to a great extent, leaves the choice of detailed approaches and procedures to the individual domain analysts. In the development of the alarm surveillance domain model, major phases of the FODA process were executed. However, a different order was used where necessary and choices in procedures and representations were made to meet the needs of the project. As such, the overriding objective was to create FODA products, modifying the process where necessary to achieve this goal.

3.5.1 The Sources of Information

Four general sources were used: domain experts, existing application systems, technical literature, and existing standards and network management and data communications.

o **Using Domain Experts to Develop Domain Products**

During the development of the domain model, the bulk of the domain expertise was obtained by interviewing domain experts in alarm surveillance. Experts with experience in developing alarm surveillance application systems are as useful or more useful than the applications themselves. They can draw on their experience and knowledge to provide information that can't be obtained from examining individual applications.

o **Using Domain Experts for Review**

During the domain analysis effort, *extensive review of the domain modeling products by experts is essential* to a successful domain modeling effort. It is also useful to

establish a secondary group of reviewers in addition to the core group of domain experts and/or application systems.

- **Using Application Systems**

  The FODA method specifies use of application systems as a basis for developing the domain model. In the alarm surveillance domain, it proved difficult to obtain a sufficient quantity of well-documented application systems. Instead, information about application systems was obtained from the domain experts. These experts were able to draw upon their knowledge of existing systems and COTS products as well as their experiences in developing systems.

- **Using Technical Literature**

  Articles, papers and other written material can be used to provide basic background for domain analysts prior to commencing domain modeling. In addition, information gained can be used to provide guidance in interviewing domain experts, allowing the domain analyst to focus on specific aspects of the domain that would not otherwise emerge during the discussion.

- **Using Standards**

  Where possible, the development was based on use of standards for data representation and information exchange. In particular, standards were particularly useful in developing the Information Model, as indicated above.

3.5.2 Order of Submodel Development

The FODA method prescribes the development of the Information Model first. The Information Model is developed first to ensure that a proper level of abstraction is established for the entire domain model. The Feature Model is developed as a second step. The Functional Model is developed last, since it is regarded as being closer to implementation than the preceding models.

In developing the alarm surveillance model, the Functional Model was begun first. The reason for this is that the alarm surveillance domain experts that supported the development effort were more accustomed to viewing their domain in terms of processes than data. Hence it was necessary to develop the Functional Model first to establish some momentum in the project. The Information Model and Feature Model were begun afterwards. However once developed, the Information Model did serve its intended purpose of helping to establish the level of abstraction for the domain model. The Feature and Functional Models were adjusted accordingly.

3.5.3 Developing the FODA Submodels

The FODA domain model could have been developed in one of two ways:

- Interview of domain experts to identify commonality in functions and data structures. This included determining what components of the models were specialized, how they were specialized, and why they were specialized. This activity was, in part, driven by detailed assessments of the impact of contextual variation in different parts of the domain model.

- The examination of knowledge about system examples to (1) identify what is commonality between known systems and (2) to distinguish differences which provide the basis for describing variabilities.

Of these two extensions to the more traditional approaches, the first predominated in the development of the alarm surveillance domain model because of the scarcity of good systems examples.

Once the initial versions of all three models were created, development proceeded in an iterative fashion with changes in one model affecting the content of the other two. Links between all three models were maintained. The development of the individual FODA models was based on examination of domain artifacts and interview of domain experts followed by review and reformulation. Knowledge gained from domain experts and other sources listed above was recorded in the evolving submodels, and the results of the interviews together with the changed models were presented to the experts for review. Their comments often elicited further changes. In addition, when one Submodel was changed, the other two were examined to see how they would have to be altered. As the feature model approached completion, specific issues were focused on, leading to smaller changes and refinements of the models.

The completed feature model was provided to a team of domain experts located at GTE Laboratories in Needham, Massachusetts, for further review. This team of experts did not participate during the domain modeling phase. Their review resulted in about 6 additions or modifications to individual features and, as such, served to validate the Feature Model directly and the domain model indirectly.

3.5.3.1 Developing the Information and Functional Models

The development of the Functional Model was based on use of IDEF0 modeling techniques. General guidelines for use of IDEF0 were provided by [APPLE88]. To more precisely define the process by which specific functions were performed, a state transition modeling approach was used that is based on Finite State Machine theory. The Information Model was developed using conventional Information Modeling approaches, supplemented by the use of Culture semantic modeling language (discussed in section 6.1). By agreement

with the domain experts, this model was based largely on the ISO/IEC standard for network management information and therefore its development was relatively straightforward.

3.5.3.2 Developing the Feature Model

The development of the Feature Model was guided, to a significant extent, by the FODA description of this process, provided in section 5.1 of [KANG90]. Additional information on how to perform this process was obtained in a seminar provided by the Software Engineering Institute in April of 1993 and by examining Domain Analysis of the Movement Control Domain [COHEN92].

FODA prescribes the development of a feature catalog, listing features of existing system examples. Because domain experts served as the primary source of domain expertise, the initial feature catalog reflected the composite knowledge of the experts rather than individual systems. Because of this, the feature catalog took the character of a more abstract "model" early and rapidly evolved into the Feature Model described in section 4. Individual system features of a catalog would correspond to the two lowest levels in the Feature Model hierarchy.

The domain analyst expended considerable effort organizing and structuring the Feature Model and in determining how the Feature Model parameterized the Functional Model. Issue/Decision descriptions were developed to accompany optional and alternative features. Specific techniques were not available for determining that all domain features and Issue/Decision descriptions had been included or for ensuring consistency between the Feature Model and the Functional and Information Models. The development of the Feature Model depended most heavily on review by domain experts since it was more unprecedented than the other two models.

3.6 The Prototype Application Development Tool

In using a domain model to develop application systems for large, complex domains, automated capabilities are needed to assist the application developer in selecting features to parameterize the Functional and Information Models. To provide the application developer with this automated assistance, the Prototype Application Development Tool was created. This Prototype Tool was developed in collaboration with the Advanced Systems Technology Corporation (ASTEC). The Tool was designed using the Culture semantic modeling language, described more fully in section 6.1 of this report. The tool was implemented using the CaMERA[4] repository system. Both the Culture language and CaMERA are products of ASTEC.

---

[4]CaMERA stands for Culture-adaptive Mechanism for Expression, Reflection, and Analysis.

The purpose of the Prototype Application Development Tool is to automate the process of deriving application system requirements through feature selection. The Prototype Tool contains an internal representation of an entire FODA domain model, including the Feature Model, Functional Model, and Information Model. Elements of these models are expressed in Culture language statements that either may be entered manually by domain analysts or imported using batch files. Relationships can be defined between individual features and components of the Functional and Information Models that describe software requirements for those features. These internally-represented relationships allow the feature model to be used to parameterize the Functional and Information Models to derive application system requirements. The Prototype Tool is generic and can be applied to any domain.

A graphical user interface (GUI) to the Feature Model is provided. This interface allows display of the hierarchy of operational features for alarm surveillance. This hierarchy is shown in the following section of this report. A mouse-driven interface can be used to scroll through the hierarchy and to highlight individual features. Mouse clicks can be used to cause detailed feature descriptions to be displayed together with information on constraints and dependencies between features. For alternative and optional features, the mouse can be used to display issue/decision information, including descriptions of rationales for selecting features. The mouse is used to select alternative and optional features; selected features are displayed in a separate window using a GUI. The selected features, together with mandatory features that are provided automatically, define the application system being developed.

Once a feature selection is complete, a program within the Prototype Tool is activated to produce application system requirements. The program uses the selected features to parameterize the Functional and Information Models represented internally within CaMERA. Internally represented links between mandatory features and selected optional and alternative features are followed. Corresponding components of the Functional and Information Models are selected and placed in an output file. This file represents functional requirements for an individual application system that was defined through feature selection. At present, the functional requirements are composed, using generic English-language statements. The underlying CaMERA repository system can be extended to generate functional requirements in other, well-known requirements languages, such as DoD-STD-2167a. The current version of the Prototype Tool does not allow for graphic representation of IDEF diagrams or entity-relationship diagrams; only the information content of these diagrams is stored and generated. Future versions of the Prototype Tool may include representation of diagrams.

The development of the Prototype Application Development Tool has demonstrated the effectiveness of both (1) the reuse of the domain model to produce application system requirements and (2) the use software systems to automatically generate software products. The Prototype Tool is available for demonstration at the Computer Systems Laboratory of the National Institute of Standards and Technology and at ASTEC. The development of the Prototype Tool has provided a basis for future research efforts in software support tools for domain engineering.

4. THE FEATURE MODEL

This section presents in detail the two components of the FODA Feature Model that have been developed for the alarm surveillance domain: context features and operational features. An overview of the major Feature Model components and a description of the hierarchical structure of the Feature Model was provided in section 3.2. The description of the Feature Models (or submodels) given below is followed by descriptions of Issues and Decisions. In the Feature Models, references are provided to Issues and Decisions that the application system developer will use to select alternative and optional operational features.

4.1 Organizational Conventions for Feature Model

The Feature Model is presented as an indented hierarchical list of features in which more general categories of features appear at higher levels. Within more general categories, more detailed levels are provided, using the FODA *consists of* aggregation relationship. Aggregated features at lower levels describe more specific capabilities. Features that are alternative or optional are so noted; otherwise the features are mandatory. In some cases, a mandatory feature may appear below an alternative or optional feature. In such cases, the mandatory feature is mandatory only if the higher-level alternative or optional feature is selected.

The indented list format was used instead of the graphical hierarchical representation found in [KANG90] and [COHEN92] because indented lists provided a representation of domain features that was more consistent with the documentation most domain experts and application developers were used to seeing. The indented list format also serves as a table of contents for the rest of this section. Page numbers for extended feature descriptions are provided in parentheses.

Feature Model Hierarchy Overview

The Feature Model can be viewed as a catalog of features for systems in the domain. The feature definitions presented below are based on the prescribed format in [KANG90]. Each definition contains the name of the feature, a short description, and an identification of the source of information about the feature. The type of the feature--whether it is mandatory, alternative, or optional--is identified. For optional and alternative operational features, those context features that affect selection of this feature are identified. The explicit identification of the affecting context feature is an extension to the feature definition format prescribed by FODA. This extension was found useful by the domain analysts and the users of the domain model and is also shown in the Issue/Decision descriptions in section 4.4. For each alternative and optional feature, a reference is provided to the relevant Issue/Decision description that should be consulted in making the selection.

With regards, to FODA feature composition rules, this domain model assumes two: *unidirectional dependency* and *mutual exclusion*. Unidirectional dependency, denoted by the term *requires*, indicates that the selection of one feature requires the selection of another feature, although the reverse may not necessarily hold true. Mutual exclusion indicates that two features cannot both be selected; this is denoted by the term *constrains*.

4.2 Context Features

This section describes in detail the context features of the alarm surveillance domain.

4.2.1 Management Architecture

Description: This feature describes the type of network management architecture for the communications network being monitored. The operational features of the alarm surveillance system will depend on the type of management architecture in existence and its position within that architecture. Three types of architectures are possible: centralized, distributed, and distributed hierarchical. These are described below.

Type: Mandatory

Source: [GTE93a], [GTE93b], and [GTE93c]

4.2.1.1 Centralized (Alternative)

Description: The alarm surveillance system is in a centralized architecture where there is one network management station.

Type: Alternative

4.2.1.2 Distributed Peer-to-Peer (Alternative)

Description: The alarm surveillance system is in a distributed architecture where it is one of several peer systems.

Type: Alternative

4.2.1.3 Hierarchical (Alternative)

Description: The alarm surveillance system is in a distributed hierarchical architecture where it may be a top, intermediate, or leaf node management station.

Type: Alternative

a) Top-Level Node (Alternative)

Description: The alarm surveillance system is the top node in a distributed hierarchical architecture. A node at this level may receive network status summary information from intermediate-level nodes and/or may directly monitor only specific very high-priority resources.

Type: Alternative

b) Intermediate-Level Node (Alternative)

Description: The alarm surveillance system is an intermediate-level node in a distributed hierarchical architecture. Intermediate nodes are between top-level and leaf-level nodes. A network management architecture may have several levels of intermediate-level nodes. A node at this level may receive network status summary information from other intermediate-level or leaf-level nodes and/or may directly monitor only specific higher-priority resources.

Type: Alternative

c) Leaf-Level Node (Alternative)

Description: The alarm surveillance system is a leaf-level node in a hierarchical architecture. At this level, network resources are monitored directly--that is, site management is performed.

Type: Alternative

4.2.2 Global Network Structural Characteristics

Description: These features define the network size (number of devices), network topology, bandwidths, and characteristics of communications equipment that affect transmission. Many of these features are quantitative scalar variables. These variables can be used in formulas to compute the maximum number of devices that can be monitored using either active or passive monitoring strategies. The particular formulas used should be selected by the domain experts in accordance with the needs of the application system being developed. The results of these computations affect the selection of operational features for monitoring. Quantitative variable features capture variability in such things as the number of network devices and the distance of these devices from the management station ("number of hops"). The variability in the values of quantitative scalar variables influences the selection of alternative and optional operational features.

Type: Mandatory

Source: [GTE93a], [NMF92a], [GTE93b], and [BEN90]

4.2.2.1 Subnetwork Characteristics

Description: This feature describes the physical characteristics of the equipment for implementing the immediate connection relationships between network resources at the local level and its relationship to the alarm surveillance system. Information for each subnetwork within the purview of the alarm surveillance system is provided.

Type: Mandatory

a) Subnetwork Number and Type

Description: This feature describes the number of subnetworks and whether the subnetwork is a local area or metropolitan area network (LAN or MAN). The feature is a quantitative scalar variable.

Type: Mandatory

b) Number of End System Devices

Description: This feature describes the number of end system devices connected to each subnetwork. The feature is a quantitative scalar variable.

Type: Mandatory

c) Number of "Hops"

Description: This feature describes the number of intermediary devices that must be traversed by each subnetwork to send a message from a device on the LAN to the alarm surveillance system. The feature is a quantitative scalar variable.

Type: Mandatory

d) Internal Bandwidth

Description: This feature describes the carrying capacity in each subnetwork in bytes/second. The feature is a quantitative scalar variable.

Type: Mandatory

4.2.2.2 Trunk/Backbone Characteristics

Description: This feature describes the physical characteristics of the wide area network (WAN) or MAN equipment for implementing trunks or backbones that connect LAN and MAN subnetworks.

Type: Mandatory

a) Trunk/Backbone Type

Description: This feature describes whether the trunk is a MAN or WAN.

Type: Mandatory

b) Bandwidth

Description: This feature describes the carrying capacity of the WAN in bytes/second. The feature is a quantitative scalar variable.

Type: Mandatory

4.2.2.3 Network Structure Alterability

Description: This context feature defines whether the overall physical organization of the network is static or can take on a finite set of different organizations. This includes changes to the content of the network (addition or deletion of subnetworks and trunks) as well as to connectivity (the changes in interconnectivity that may occur as a result of the addition or deletion of trunks or backbones).

Type: Mandatory

Source: [GTE93b]

a) Static (Alternative)

Description: The network structure does not change.

Type: Alternative

b) Variable (Alternative)

Description: The network structure may take on different organizations. Each different organization may consist of different subnetworks and subnetwork characteristics and different set of trunk/backbones and trunk/backbone characteristics. These different organizations may be associated with different operating modes.

Type: Alternative

Requires: Variable Resource Characteristic Alterability

4.2.3 Individual Network Resource Characteristics

Description: These features describe the characteristics of managed resources (both network devices and agents) that lie within the communications network. These characteristics include the criticality of the function of the network devices to the overall mission of the communications network and the organization it supports, the types of event notifications emitted by network resources, and the management protocols used. The selection of optional and alternative context features for network resources should reflect the aggregate characteristics of all the network resources to be managed.

Type: Mandatory

4.2.3.1 Resource Criticality Rank (Optional)

Description: This context feature allows the characterization of "criticality" of network resources within a managed network.

Type: Optional

Source: [GTE93a] and [GTE93b]

a) **Ranking Scheme Types**

Description: The criticality of network resources to a communications network may be ranked according to several different schemes. Within different schemes, the extent of variability of various ranking levels is too great to be captured here.

Type: Mandatory

a.1) **Mission Criticality (Optional)**

Description: The resources within the managed network (or subdivision thereof) provide mission-critical services.

Type: Optional

a.2) **User Groups (Optional)**

Description: Resources in the managed network (or subdivision thereof) may be classified on the basis of what user groups they belong to.

Type: Optional

a.3) **Security Levels (Optional)**

Description: Resources in the managed network (or subdivision thereof) may be classified on the basis of the security level of the messages they transmit.

Type: Optional

a.4) **Device Types (Optional)**

Description: Resources in the managed network (or subdivision thereof) may be classified on the basis of the type of device.

Type: Optional

b) **Number of Devices at Scheme Levels**

Description: This feature allows the expression of the number of devices at each level within a particular ranking scheme. The feature is a quantitative scalar variable.

Type: Mandatory

4.2.3.2 Management Protocol Used

Description: This context feature describes the management protocols responded to by agents within the management network.

Type: Mandatory

Source: [GTE93b]

a) Standard Management Protocol

Description: These features describe the standard management protocols that may be responded to by agent systems. (Please note: this is a situation that cannot be easily expressed using alternative or optional features--at least one but also more than one protocol alternatives may be selected).

a.1) SNMP (Alternative)

Description: The protocol responded to by agents is SNMP.

Type: Alternative

a.2) SNMP v2 (Alternative)

Description: The protocol responded to by agents is SNMP v2 (version 2).

Type: Alternative

a.3) CMIP/CMIS (Alternative)

Description: The protocol responded to by agents is CMIP/CMIS.

Type: Alternative

b) Proxy Proprietary Management Protocol (Optional)

Description: These features describe the proprietary management protocols that may be responded to by agent systems via a proxy device. (Please note: this is a situation that cannot be easily expressed using alternative or optional features--at least one but also more than one protocol alternatives may be selected).

b.1) SNMP Proxy (Alternative)

Description: The proprietary protocol responded to by agents via a proxy mechanism is SNMP.

Type: Alternative

b.2) SNMP v2 Proxy (Alternative)

Description: The proprietary protocol responded to by agents via a proxy mechanism is SNMP v2.

Type: Alternative

b.3) CMIP/CMIS Proxy (Alternative)

Description: The proprietary protocol responded to by agents via a proxy mechanism is CMIS/CMIP.

Type: Alternative

c) Resource Characteristic Alterability

Description: This context feature defines whether the aggregate resource characteristic descriptions remain static or can change. This includes changes to whether or not Resource Criticality Rankings can change, which particular Resource Criticality Rankings exist, and what Management Protocols used. The changes to the aggregate resource descriptions are brought on by the addition or deletion of network resources.

Type: Mandatory

Source: [GTE93b]

c.1) Static (Alternative)

Description: Aggregate resource characteristic descriptions remain static.

Type: Alternative

c.2) Variable (Alternative)

Description: Aggregate resource characteristic descriptions can change.

Type: Alternative

Requires: Variable Network Structure Alterability

4.2.4 Communications Network Operating Modes (Optional)

Description: These features define operating modes that a communications network may assume. Operating modes are particular states a network may be in, such as peacetime or wartime. Four categories of modes are defined as optional context features: daily operating modes, contingent modes, military modes, and reconstitution modes. The communications network may assume one particular mode at any time (i.e., it may be in a daytime, non-contingent, crisis, non-reconstituting mode). The ability of the alarm surveillance system to respond to these modes will be determined by the selection of specific optional and alternative operational features.

Type: Optional

4.2.4.1 Daily Operating Modes (Optional)

Description: This feature describes operating modes a network may be in during the course of routine or usual activity.

Type: Optional

Source: [GTE93b]

a) Daytime/Business

Description: The communications network is operating during normal "business" hours.

Type: Mandatory

b) After Hours

Description: The communications network is operating after normal "business" hours. This is the so-called "lights out" mode.

Type: Mandatory

4.2.4.2 Contingency Modes (Optional)

Description: This feature describes the modes that denote the absence or existence of a contingency situation on the network. A contingency situation may mean that a portion of the communications network is not receiving normal alarm surveillance services (i.e., another station may have gone down) or that the services provided are severely degraded.

Type: Optional

Source: [GTE93b]

a) Non-Contingent

Description: The communications network is operating without a contingency situation.

Type: Mandatory

b) Contingent

Description: The communications network is operating in a contingency mode. In response to this mode, the alarm surveillance system may need to monitor additional parts of the network.

Type: Mandatory

4.2.4.3 Military Modes (Optional)

Description: This feature describes the military operating modes pertaining to survivability requirements.

Type: Optional

Source: [GTE93a] and [GTE93b]

a) Peace

Description: The communications network is in a "peacetime" mode.

Type: Mandatory

b) Crisis

Description: The communications network is in a "crisis" mode.

Type: Mandatory

c) War

Description: The communications network is in a "wartime" situation.

Type: Mandatory

d) Training/Exercise

Description: The communications network is undergoing training exercises.

Type: Mandatory

4.2.4.4 Reconstitution Modes (Optional)

Description: This feature describes whether or not the communications network is in a process of reconstituting itself. A network that has been partially destroyed as a result of war or other natural or manmade disasters may have to be reconstructed.

Source: [GTE93a] and [GTE93b]

a) Non-Reconstituting

Description: The communications network is not in the process of reconstituting itself.

Type: Mandatory

b) Reconstituting

Description: The communications network is in the process of reconstituting itself.

Type: Mandatory

4.2.4.5 Bursty Traffic Mode (Optional)

Description: This feature describes situations in which the communications network experiences a sudden upsurge in communications traffic that degrades, or threatens to degrade, the overall performance of the network. Bursty traffic situations may occur for many reasons, including the sudden transfer of large amounts of multimedia information or the redundant reporting of the same fault by many agents.

Source: [GTE93b] and [GTE93c]

4.2.5 Staffing Requirements

Description: This category of features describes requirements for staffing the network management station. The existence of staffing restrictions leads to selection of optional features associated with increased automation of alarm surveillance capabilities. The feature is a quantitative scalar variable.

Type: Mandatory

Source: [GTE93a]

4.3 Operational Features

The operational features of the alarm surveillance subdomain are listed below. With regards, to FODA feature categorization, all features are *compile-time* features.

4.3.1 Monitoring

Description: Monitoring is the process of gathering information about faults and fault-related conditions that have occurred or that may occur within a communications network. Monitoring features allow the network administrator to define the part of the network and the set of network resources that will be monitored. This is called defining the scope of responsibility. These features allow the organization of the network resources within that scope into different groups for monitoring purposes. The features also allow determination of the method by which information is gathered, known as the monitoring strategy, for all or part of the communications network.

4.3.1.1 Monitoring Scope Definition and Control

Description: The scope of the managed network is determined by the set of network resources to be monitored. These features allow the definition and control of the scope of the communications network that will be monitored.

Type: Mandatory

a) Select Alternative Monitoring Organization

Description: Allows network administrator to determine whether the managed network will be monitored as one unit or be partitioned into subsets that can be monitored separately.

Type: Mandatory

Source: [GTE93b]

a.1) Consolidated (Alternative)

Description: Specifies that network will be monitored as one unit or segment.

Type: Alternative

Affecting Context Features: (1) Physical characteristics, (2) Resource Criticality Rank, (3) Operating Modes, and (4) Variable Network Alterability

a.2) **Partitioned (Alternative)**

Description: Allows network to be partitioned into separate partitions that can be monitored using different monitoring strategies--or in the case of polling, to be monitored using different polling time intervals. (See below.) The feature allows the network administrator to place network devices into different partitions together with device addresses and other device-specific information.

Type: Alternative

Affecting Context Features: (1) Physical characteristics, (2) Resource Criticality Rank, and (3) Operating Modes

a.2.1) **Define Network Partition**

Description: This feature allows a network partition to be defined and to have network resources (devices) associated with it.

Type: Mandatory

a.2.2) **Enable/Disable Network Partition**

Description: This feature allows the operation of a network partition to be enabled or disabled.

Type: Mandatory

b) **Define Scope of Responsibility**

Description: Allows specification of what resources will be monitored and the entry of necessary configuration information about those resources.

Type: Mandatory

b.1) **Scope Definition and Enforcement Mechanism**

Description: This feature provides two alternative ways for the network administrator to define and control the scope of responsibility.

Type: Mandatory

Source: [GTE93b]

b.1.1) **Administrative Responsibility Profiles (Alternative)**

Description: Allows definition of filtering constructs that specify what devices are inside or outside the scope of responsibility of the alarm surveillance system. Filtering constructs take the form of patterns that must be matched (or not matched) by incoming event notifications.

Type: Alternative

Affecting Context Features: (1) Management Protocol Used, (2) Global Network Structural Characteristics, and (3) Network Policy

b.1.2) **Network Device SET Commands (Alternative)**

Description: Allows definition of scope of responsibility through SET commands that alter internal variables that specify where an agent for a network device forwards event notifications.

Type: Alternative

Affecting Context Features: (1) Management Protocol Used, (2) Global Network Structural Characteristics, and (3) Network Policy

b.2) **Method of Configuration Data Entry**

Description: Allows entry of network configuration data necessary for monitoring network resources through polling or alarm generation. This data includes the device identification, device addresses and other device specific information. The data may be entered for individual devices or for entire network partitions (also referred to as management domains) if in a partitioned monitoring organization. (See Partitioned Monitoring Organization below.)
Type: Mandatory

Source: [GTE93b]

b.2.1) **Manual Entry**

Network configuration data may be entered manually either through a user interface or by loading of a batch file.

Type: Mandatory

b.2.2) **Automatic Entry (Optional)**

Network configuration data may be entered automatically by the configuration management component of a network management system, possibly as a result of a "self-discovery" operation.

Type: Optional

Affecting Context Features: (1) Network Structure Alterability, (2) Resource Characteristic Alterability, and (3) Existence of Communications Network Operating Modes context features

b.3) **Dynamic Scope Increase/Decrease (Optional)**

Description: Allows definition of actions by the network administrator that allow dynamic run-time addition of network resources to be monitored. These actions are defined to take place automatically. The added network resources would normally fall within the scope of responsibility of another manager system that has failed. The ability to dynamically increase scope should be accompanied by the complimentary ability to decrease scope by dynamically removing network devices from the scope of responsibility of a particular alarm surveillance system.

Type: Optional

Affecting Context Features: (1) Network Structure Alterability, (2) Resource Characteristic Alterability, (3) Distributed Hierarchical or Peer-to-Peer Management Architecture, and (4) Bursty Traffic Mode

Requires: Automatic Configuration Data Entry, Partitioned monitoring organization.

Source: [GTE93b]

b.3.1) **Receive Scope Increase/Decrease**

Description: Allows alarm surveillance station to be the recipient of a scope increase/decrease action initiated by a remote station.

Type: Mandatory

b.3.2) **Initiate Scope Increase/Decrease**

Description: Allows alarm surveillance station to initiate a scope increase/decrease action that will effect a remote station.

Type: Mandatory

4.3.1.2 Monitoring Strategy Definition and Control

Description: The selection of monitoring strategy determines how the managed network is to be monitored including: types of messages sent, frequency of message transmission, and the extent to which to control of the polling process can be automated.

Type: Mandatory

Source: [GTE93a] and [BEN90]

a) **Define Polling Message**

Description: Allows network administrator to define the poll message as either a PING-type or GET operation. The selection of both alternatives should also be allowed. (Please note: this is a case where the FODA feature types--Alternative and Optional--do not completely capture the kinds of choices that may be made. Perhaps another feature type is required that allows selection of more than one alternative.)

Type: Mandatory

Rules: At least one of either a.1) PING-type or a.2) GET-type must be selected. Both may be selected.

Source: [GTE93b]

a.1) **PING-type (Optional)**

Description: Allows selection of PING-type message. If the device agent is operational, it will respond with an acknowledgement--a "PONG."

Type: Optional

Affecting Context Feature: Global Network Structural Characteristics

a.2) **GET-type (Optional)**

Description: Allows selection and definition of GET-type message to retrieve values of selected variables that indicate the device's status. This option is needed to obtain data for computation of fault "health index" function.

Type: Optional

Affecting Context Features: (1) Global Network Structural Characteristics and (2) Network Management Architecture

b) **Polling Control**

Description: This group of features describe the controls the network administrator has over the polling of the communications network. (Please note: it is recognized that polling is a separate functional area from alarm surveillance. As such, polling is used equally by performance management,

configuration management, and fault management (including alarm surveillance). However, it is necessary to describe polling features for alarm surveillance, since polling network resources to detect faults has unique requirements. Within the Functional Model, polling functions are included to provide a complete picture.)

Type: Mandatory

Source: [GTE93b]

b.1) **Manual Polling**

Description: Allows initiation of manual polls of individual devices or sets of devices.

Type: Mandatory

b.2) **Automatic Polling**

Description: Allows devices to be monitored automatically.

Type: Mandatory (but could be optional)

b.2.1) **Set Polling Time Interval**

Description: Allows network administrator to control the Polling Time Interval (PTI).

Type: Mandatory

b.2.1.1) **Manual Polling Time Interval Control**

Description: Allows setting polling time interval manually.

Type: Mandatory

b.2.1.2) **Automatic Polling Time Interval Control (Optional)**

Description: Allows setting parameters of Automatic Polling Time Interval (PTI) Adjustment Algorithm, such as the rate at which the PTI may change.

Type: Optional

Affecting Context Features: Staffing

b.2.2) **Partitioned Polling Time Interval Scope (Optional)**

Description: Allows specification of whether a Polling Time Interval can be set for individual partitions.

Type: Optional

Affecting Context Features: See Partitioned alternative for Monitoring Organization

Requires: Partitioned Monitoring Organization

b.2.3) **Individual Device (Optional)**

Description: Allows specification of whether a Polling Time Interval can be set for individual devices.

Type: Optional

Affecting Context Features: (1) Resource Criticality Rank (the existence of a small number of very high priority devices) and (2) Network Operating Modes

4.3.1.3 Set Alarm Thresholds (Optional)

Description: This feature allows the network administrator to remotely set or reset threshold levels for alarm notifications maintained by agent systems. This includes thresholds for particular types of alarm notifications maintained by agent systems for many resources as well as thresholds maintained by an agent system for an alarm notification on a particular network resource.

Type: Optional

Source: [GTE93b] and [GTE93c]

Affecting Context Features: (1) Resource Criticality Rank (the existence of network resources having different levels of priority), (2) Network Operating Modes, and (3) Global Network Structural Characteristics

4.3.2 Filtering

Description: Filtering features allow the network administrator to control the distribution of event notifications describing faults. Filtering screens out redundant or irrelevant notifications. Together with analysis features described in section 4.3.3, filtering features assist the network administrator in ensuring that (a) genuine reports are sent to appropriate destinations, and (b) the resources of the communications network are directed toward the most critical faults. The features described below allow the network administrator to define constructs for event notification filtering and to control their operation.

Type: Mandatory

4.3.2.1 Event Profile Definition

Description: This feature allows the definition of event profile filtering constructs (creating a pattern to match event profiles). Event profiles are used to filter event notifications that pertain to faults affecting the operation of the network. Filtering profiles may be defined to take one of several actions described below.

Type: Mandatory

Source: [GTE93b], [ISO/IEC 10164-5], and [NMF92b]

a) Definable Filtering Actions

Description: This feature defines the actions that can be specified in an event profile.

Type: Mandatory

a.1) Forward High-Priority Notification to Remote Destination

Description: Allows network administrator to specify the address of communicating entity to which a high-priority event notification should be forwarded. This includes both reported and cleared alarms.

Type: Mandatory

a.2) Discard Event Notification (Filter Out)

Description: Allows network administrator to specify that a particular kind of event notification should be discarded and filtered out.

Type: Mandatory

a.3) Retain Event Notification for Further Analysis

Description: Allows network administrator to specify that a particular kind of event notification should be forwarded to Function **Analyze Events** for further analysis.

Type: Mandatory

b) **Remote Filtering Location (Optional)**

Description: Allows network administrator to locate event profiles within the device agent.

Type: Optional

Affecting Context Features: (1) Management Protocol Used, (2) Global Network Structural Characteristics, (3) Network Operating Modes, and (4) Network Policy

4.3.2.2 Filtering Operation Control

Description: This feature allows the network administrator to control operation of various aspects of filtering system.

Type: Mandatory

Source: [ISO/IEC 10164-5] and [NMF92b]

a) **System Control**

Description: This feature allows the network administrator to enable and disable the operation of the entire filtering system; i.e., to turn it on and off.

Type: Mandatory

b) **Event Profiles**

Description: This feature allows the network administrator to enable and disable the operation of an individual Event Profile; i.e., to turn it on and off.

Type: Mandatory

c) **Event Profile Sets (Optional)**

Description: This feature allows the definition and control of sets of event profiles, called event profile sets. Using this feature, the network administrator may place into one set those event profiles that should be used together for particular operating mode, such as a particular military mode and contingency mode. Event Profiles may also be grouped to create event profile sets that are specific to intermediate or leaf-level node managers. Particular event profile sets may be enabled or disabled depending on the mode or role the alarm surveillance system is called upon to play.

Type: Optional

Affecting Context Features: 1) Operating Modes; 2) Network management architecture, (3) Variable Network Alterability, and (4) Resource Criticality Rank

Source: [GTE93b]

c.1) **Event Profile Set Definition**

Description: This feature also allows creation and deletion of construct sets. The network administrator may also add or remove individual event profiles from sets.

Type: Mandatory

c.2) **Enable/Disable Event Profile Set (Optional)**

Description: This feature allows the network administrator to enable and disable the operation of an event profile set; i.e., to turn it on and off.

Type: Optional

Affecting Context Features: (1) Global network structural Characteristics and (2) Bursty Traffic Mode

d) Event Profile-Partition Association (Optional)

Description: This feature allows the specification that individual event profiles can be associated with network partitions (also referred to as management domains) in a partitioned organization.

Type: Optional

Affecting Context Features: Operating modes

Source: [GTE93b]

d.1) **Individual Construct Association (Alternative)**

Description: This feature allows the specification that individual event profiles can be associated with network partitions (management domains) in a partitioned organization.

Type: Alternative

Requires: Partitioned Monitoring Organization

d.2) **Set Association (Alternative)**

Description: This feature allows the specification that event profile sets can be associated with network partitions in a partitioned organization.

Type: Alternative

Requires: Partitioned Monitoring Organization, Event Profile Sets

4.3.3 Analysis

Description: Analysis is directed toward the event notifications received by the alarm surveillance system. The purpose of analysis activity is to identify alarms that describe faults

that are affecting, or will affect, the operation of the network. Analysis works with filtering. By identifying genuine alarms, analysis activity implicitly performs a filtering function. The results of analysis activity may also be used to identify notifications that are no longer relevant and should be filtered out. The features described below allow the network administrator to control the definition and operation of constructs that can be used by the alarm surveillance system to perform analysis. These constructs are stated as condition-action rules that interpret poll responses to identify alarm situations, correlate event notifications to identify actual sources of alarms, and automatically determine disposition of outstanding alarm notifications.

Type: Mandatory

4.3.3.1 Analysis Construct Definition

Description: These features allow definition of constructs that can be used to analyze incoming event notifications. Following established conventions in this domain, these constructs take the form of expert system rules that have condition and action parts. Rules can be defined to correlate different types of event notifications, specify if correlated event notifications should be reported, or analyze polling responses to identify alarm conditions.

a) Define Correlation Rule

Description: This feature allows network administrator to define condition and action patterns for correlation rules. This includes the definition of rules with condition and action statements that are specifically designed to enable correlation of event notifications. For instance, a condition statement may be defined for an arbitrarily large count of occurrences as a threshold in the antecedent of the rule.

Type: Mandatory

Source: [GTE93] and [JAKOB93]

b) Define Alarm Disposition Rule

Description: This feature allows network administrator to define condition and action patterns for alarm disposition rules. These rules are necessary to determine what to do with event notifications that have been correlated (or that cannot be correlated). The condition parts of the rule should allow definition of patterns that are specifically designed to match asserted correlations. Disposition rules allow specification of actions that enable the operations described in the subfeatures below. The information content of the messages specified by these actions is described in entity definitions in the entity relationship model. In the rule definitions, each message appears as a pattern that can be instantiated.

Type: Mandatory

Source: [GTE93b] and [ISO/IEC 10164-5]

b.1) **Report Alarm Action**

Description: This feature allows rule actions to be defined for reporting alarms to remote destinations.

Type: Mandatory

b.2) **Clear Alarm Action**

Description: This feature allows rule actions to be defined for clearing an alarm and for forwarding notice of this action to a remote destination.

Type: Mandatory

b.3) **Issue Follow-Up Manager Inquiry Action**

Description: This feature allows rule actions to be defined for issuing a follow-up manager inquiry that is forwarded to an agent system.

Type: Mandatory

b.4) **Issue Alarm Disposition Unknown Message**

Description: This feature allows rule actions to be defined for clearing an alarm and for forwarding notice of this action to a remote destination.

Type: Mandatory

b.5) **Enable/Disable Event Profile Action (Optional)**

Description: Allows specification of the activation and deactivation of an event profile. The activation action is designed to filter alarms that have already been correlated and do not need to be reported again. Deactivation may be necessary after correlated and reported alarms have been cleared.

Type: Optional

Affecting Context Features: Global Network Structural Characteristics

Source: [GTE93b]

c) **Define Polling Analysis Rule**

Description: Allows definition polling analysis rules for analysis of poll responses.

Type: Mandatory

Source: [GTE93b]

4.3.3.2 Construct Operation Control

Description: This feature allows the network administrator to control operation of analysis rules and analysis construct sets.

Type: Mandatory

a) **Individual Analysis Construct Control**

Description: This feature allows network administrator to enable or disable the operation of individual analysis rules; i.e., to turn the rules on or off.

Type: Mandatory

Source: [GTE93b]

b) **Analysis Construct Set Control (Optional)**

Description: This feature allows the definition and control of sets of analysis constructs, called analysis construct sets, that can be treated as a group. These sets are analogous to event profile sets described above. Using this feature, the network administrator may place into one set those analysis rules that should be used together for particular operating modes, such as a particular military mode and contingency mode. Analysis constructs may also be grouped to create construct sets that are specific to intermediate or leaf-level node managers. Particular construct sets may be enabled or disabled depending on the mode or role the alarm surveillance system is called upon to play.

Type: Optional

Affecting Context Features: (1) Operating modes, (2) Network management architecture, and (3) Variable Network Alterability

Source: [GTE93b]

b.1) **Define Analysis Construct Set**

Description: This feature allows creation and deletion of construct sets. The network administrator may also add or remove individual analysis constructs from sets.

Type: Mandatory

b.2) **Enable/Disable Analysis Construct Set**

Description: This feature allows network administrator to enable or disable the operation of an analysis construct set; i.e., to turn the construct set on or off.

Type: Mandatory

c) **Analysis Construct-Partition Association (Optional)**

Description: This feature allows the specification that individual analysis constructs can be associated with network partitions (also referred to as management domains) in a partitioned organization.

Type: Optional

Affecting Context Features: Communications Network Operating modes

Source: [GTE93b]

c.1) **Individual Construct Association (Alternative)**

Description: This feature allows the specification that individual analysis rules can be associated with network partitions (management domains) in a partitioned organization.

Type: Alternative

Requires: Partitioned Monitoring Organization

c.2) **Set Association (Alternative)**

Description: This feature allows the specification that analysis construct sets can be associated with network partitions in a partitioned organization.

Type: Alternative

Requires: Partitioned Monitoring Organization, Event Profile Sets

4.3.3.3 Network Status Summary Reporting (Optional)

Description: These features allow the definition and control of reporting capabilities for producing summary information about the state of a managed network. Features to provide three kinds of reporting capabilities are described below: (1) reporting of statistical summaries, (2) computation of a network "health index" that provides a rough measure of the criticality of faults occurring on the network, and (3) a summary of the availability of network resources within a particular network. To accumulate the information necessary to produce all three categories of reports, GET-type polling is required.

Type: Optional

Requires: GET-type polling message

a) **Compute Statistical Summary Report (Optional)**

Description: This feature allows definition and control of reports that summarize the frequency of occurrence of particular types of event notifications over specified time intervals. An example would be a report of the number of alarms occurring on a

subnetwork in successive time intervals to show a trend. The presentation of this information is defined using FODA representational features (omitted in this report).

Type: Optional

Affecting Context Features: Network Management Architecture

Source: [GTE93b] and [GTE93c]

b) **Compute Fault "Health Index" (Optional)**

Description: Allows the accumulation of selected statistical information obtained from network resources and the definition of a function for the computation of a summary "health index" that represents an aggregate measure of the networks status with respect to faults and fault-related conditions. The function is highly variable and system dependent. Two variants exist. The "health index" may be computed on the basis of percentage of reachable nodes on its network. The "health index" may also be based on such variables as the throughput delay in receiving poll responses, the utilization rate of network resources, or the error rates of resources. This feature requires accumulation of statistical information obtained from selected variables maintained within network resources. This statistical information is obtained through GET-type polling. The function may be invoked at a predetermined time interval and the results forwarded to selected destinations. The function may be defined to emit an alarm notification if a certain threshold is exceeded.

Type: Optional

Affecting Context Features: (1) Network Management Architecture and (2) Global Network Structural Characteristics

Source: [GTE93b] and [GOLD93]

c) **Compute Network Resource Availability Summary (Optional)**

Description: This feature allows definition of a reporting function that provides a summary of network devices (and other resources) within the scope of a particular alarm surveillance station that are currently available or that are "down." The summary could be limited to subsets of more critical devices and could also indicate other information such as the priority-level of devices that are "down" or the length of time devices have been available or "down."

Type: Optional

Affecting Context Features: (1) Network Management Architecture and (2) Resource Criticality Rank

Source: [GTE93b] and [GTE93c]

4.3.4 Dynamic Surveillance Control (Optional)

Description: These features allow the network administrator to program and control automatic, run-time, coordinated changes in monitoring, filtering, and analysis activity to meet changes in the communications network environment. These features are intended to satisfy requirements for responding to planned or unplanned contingency situations, to support military survivability strategies and planning, and to implement "lights out" policies. These features allow the capability to program automatic, coordinated changes in scope of responsibility, in monitoring organization, and in the monitoring strategy used. The capability also includes automatic and simultaneous activation and deactivation of filtering and analysis constructs and construct sets that will be necessary for the new network situation. The feature may require use of partitioned monitoring organization and the association of specific constructs (both filtering and analysis) or construct sets with individual partitions.

Type: Optional

Requires: For this feature to be selected, at least one of the following must be selected--Dynamic Mode Change Response, Contingency Mode Change Response, or Scheduling.

4.3.4.1 Scheduling (Optional)

Description: Allows Network Administrator to schedule automatic changes in monitoring strategy, monitoring scope and to automatically interchange filtering and analysis constructs and construct sets. Automatic changes in monitoring strategy may be applied to either consolidated or partitioned organizations. These changes may be scheduled to meet the requirements of an "after hours" or "lights out" policy.

Type: Optional

Affecting Context Features: (1) Daily Operating Modes, (2) Staffing, and (3) Network Size

Requires: Dynamic Scope Increase/Decrease, Analysis Construct Partition Association, Event Profile Partition Association

Source: [GTE93b] and [ISO/IEC 10164-5]

4.3.4.2 Dynamic Mode Change Response (Optional)

Description: Allows the Network Administrator to program a set of automatic, coordinated changes in the surveillance of the network. These changes will be programmed to occur together in response to changes in military modes, contingency modes, or reconstitution modes. Specifically, the changes may encompass any or all of the following:

- o the scope of the network being monitored--through dynamic addition of new partitions (formerly in the purview of other stations) or removal of active partitions.
- o the monitoring strategy--polling time intervals for partitions and polling messages.
- o the interchange of Event Profiles or Event Profile Sets.
- o the interchange of analysis constructs or construct sets.
- o the operation of schedules (see 4.3.4.1).

Examples of situations where these changes are desirable include the following:

1. A contingent situation may arise if a network manager becomes unavailable. In response, another alarm surveillance capability activates preprogrammed changes. These changes include assuming responsibility over the failed manager's part of the network by dynamically adding new partitions of network resources. Particular filtering and analysis constructs or construct sets are activated and used for the added partitions.

2. A transition from peace to crisis, or from peace to war, may involve changes in the scope of responsibility for individual managers as well as changes in monitoring strategy. A new set of partitions may have to be activated to replace an existing set. The new set of network partitions may reflect a different prioritization of network resources in receiving monitoring services. Partitions with higher priority resources may be monitored with more frequent polling time intervals. Particular filtering and analysis construct sets may be activated and used for the added partitions.

3. This circumstance concerns the existence of Network Structure Alterability and Resource Characteristic Alterability. Networks whose configuration and content may suddenly change for other reasons may need programmed change responses to deal with new situations.

Type: Optional

Source: [GTE93b]

Affecting Context Features: (1) Contingency Modes, (2) Military Modes, (3) Reconstitution Modes, (4) Resource Criticality Rank, (5) Network Structure Alterability, and (6) Resource Characteristic Alterability

Requires: Dynamic Scope Increase/Decrease, Analysis Construct Partition Association, Event Profile Partition Association

4.4 Issues and Decisions in Selecting Operational Features

This section presents issues and decisions used during selection of alternative and optional operational features.

4.4.1 Format of Issue/Decision Descriptions

Each issue/decision description consists of the name of the issue, a description of the issue, the name of the optional or alternative feature at which the issue was raised, and an identification of the decisions that can be made on the issue. For alternative features, each alternative decision description contains a rationale for making the decision with the affecting context feature underlined. For optional features, the decisions to select the feature are similarly documented. Decisions for not selecting an optional feature are also documented. Feature constraints and requirements are described in section 4.3. Components of the Functional Model that are parameterized by the feature selection are identified with the notation "Determines."

4.4.2 Issues in Monitoring Features

This section describes the following issues:

- Select Alternative Feature: Monitoring Organization
- Select Alternative Feature: Scope Definition and Enforcement Mechanism
- Select Optional Feature: Automatic Entry of Configuration Data
- Select Optional Feature: Scope Increase/Decrease
- Select Optional Feature: PING-Type Polling
- Select Optional Feature: GET-Type Polling
- Select Optional Feature: Automatic Polling Time Interval Control
- Select Optional Feature: Partitioned Polling Time Interval Scope
- Select Optional Feature: Individual Polling Time Interval Scope
- Select Optional Feature: Set Alarm Thresholds

ISSUE: SELECT ALTERNATIVE FEATURE: MONITORING ORGANIZATION

Description: Two alternative organizations exist: consolidated or partitioned. A consolidated organization means the network will be monitored as one unit. Partitioned organization allows the network to be divided into partitions, each that can be monitored using different monitoring strategies.

Raised at: Feature 4.3.1.1 (a)

Decision: Select Consolidated Organization

Rationale: (1) Global Network Structural characteristics and (2) Resource Criticality Rank. This alternative should be selected when there are a modest number of resources to be monitored and/or there is lack of important differences in the criticality of resources.

Determines: Specialization of function **Control Network Partition** into **Control Single Network Partition**, **Form Polling Messages** into **Form Messages for Consolidated Organization**, and **Initiate Polling** into **Initiate Consolidated Polling.**

Decision: Select Partitioned Organization

Rationale: (1) Global Network Structural characteristics. Large network size (number of devices) and bandwidth restrictions may necessitate partitioning network into parts that can be monitored separately. (2) Resource Criticality Rank. The existence of resource criticality rankings may necessitate that network resources be partitioned into subsets on the basis of prioritization criteria. Each subset should then be monitored separately using different polling time intervals characteristics. (3) Communications Network Operating Modes. During war or crisis modes, the network may have to be partitioned into subparts, each having different priorities for alarm surveillance services. Each mode may have associated with it a different set of network partitions (management domains). In addition, the existence of contingency modes may result in the run-time addition of additional partitions that would normally be monitored by management stations that have failed. The existence of daily operating modes may require that during "lights out," additional partitions must be monitored that normally belong to management stations that have become inoperable. (4) Variable Network Alterability. A network that can take on a finite number of different physical organization may require the definition of different partitions for each physical organization.

Determines: Specialization of function **Control Network Partition** into **Control Multiple Network Partitions**, **Form Polling Messages** into **Form Messages for Partitioned Organization**, and **Initiate Polling** into **Initiate Partitioned Polling.**

ISSUE: SELECT ALTERNATIVE FEATURE:
SCOPE DEFINITION AND ENFORCEMENT MECHANISM

Description: The issue addresses whether the monitoring scope of the network is to be defined and enforced through the use of administrative profiles to filter incoming event notifications or through automatic or semi-automatic commands to "SET" values of device variables.

Raised at: Feature 4.3.1.1 (b-1)

Decision: Administrative Responsibility Profiles

Description: The use of administrative profiles to filter incoming event notifications is selected.

Rationale: (1) Management Protocol Used: This alternative may be selected if the management protocol does not easily support the use of SET commands or if it is difficult and costly to write "program scripts" for each device. (2) Global Network Structural Characteristics: This alternative may be selected if the additional traffic generated through the use of SET commands would overburden the network. (See below.) (3) The use of administrative filtering should be consistent with administrative policies for network management.

Determines: Specialization of **Control Scope of Responsibility** into **Perform Administrative Filtering.**

Decision: Network Device SET Commands

Description: Use of automatic or semi-automatic commands to SET values of device variables is selected.

Rationale: (1) Management Protocol Used: The protocol must support the ability to encode and transmit "set" internal device variables. (2) Global Network Structural Characteristics: The additional traffic generated must not result in degradation of overall performance for a communications network, given network size (number of devices), bandwidth capacities, and network topology. (3) The use of SET commands should be consistent with administrative policies for network management of the organization for which the application system is being developed.

Determines: Specialization of **Control Scope of Responsibility** into **Execute Network Device SET Commands.**

ISSUE: SELECT OPTIONAL FEATURE:
AUTOMATIC ENTRY OF CONFIGURATION INFORMATION

Description: Selection of this feature allows network configuration data to be entered automatically by the configuration management component of a network management system, possibly as a result of a "self-discovery" operation.

Raised at: Feature 4.3.1.1 (b-2)

Decision: Select feature.

Rational: (1) Network Structure Alterability and Resource Characteristic Alterability. Periodic run-time changes in the configuration of the network and to the devices to be monitored necessitates the ability to receive files describing new configurations. To facilitate the operation of the network, these files must be received automatically. Manual entry would be too slow and cumbersome. (2) Communications Network Operating Modes context feature (including any of the four subfeatures). To quickly respond to dynamic changes in operating modes--particularly in military and contingency modes--will necessitate the ability to automatically load new configuration data.

Determines: Selection of feature will affect composition of the domain architecture. The domain model will not be affected.

Decision: Do not select feature.

Rational: The rationale for not selecting the feature is that the network structure would be expected to remain static; communications operating modes do not exist.

ISSUE: SELECT OPTIONAL FEATURE: SCOPE INCREASE/DECREASE

Description: The issue addresses the selection of a feature that will allow addition of sets of network resources to be monitored during contingency situations.

Raised at: Feature 4.3.1.1 (b-3)

Decision: Select feature

Rationale: (1) The existence in the context of the features Network Structure Alterability and Resource Characteristic Alterability

indicates that there will be run-time changes in the content and configuration of the managed network. This feature will be needed to respond to these changes. This feature is also required to support the optional feature **Dynamic Mode Change Response**. See the Issue/Decision description for that feature: it should be noted that the existence of military modes, contingency modes, and daily operating modes may require the dynamic (run-time) addition of additional network partitions (also referred to as management domains) that are normally monitored by other management stations. For instance, during contingency modes, additional partitions are added that would normally be monitored by management stations that are "down." The existence of daily operating modes may require that during "lights out," additional partitions must be monitored that normally belong to management stations that have become inoperable. (2) The existence of "Bursty" Traffic Mode may require temporary decreases in scope.

Determines: The data flow **Dynamic partition addition** into the function **Control Scope of Responsibility**.

Decision: Do not select feature

Rationale: The operating modes described above are not relevant to the application being developed.

ISSUE: SELECT OPTIONAL FEATURE: PING-TYPE POLLING MESSAGE

Description: The issue concerns selection of PING-type polling message.
Raised at: Feature 4.3.1.2 (a.1)

Decision: Select feature

Rationale: PING-type polling involves short, simple messages that are used to check only the operational status of network devices; i.e., if it is up or down. Global Network Structural Characteristics. Large network size (a large number of devices), bandwidth restrictions, and characteristics of network topology may require selection of this type of polling.

Determines: Specialization of Function **Form Polling Messages** into **Form PING-type Polling Messages for Consolidated Organization.**

Decision: Do not select feature

Rationale: The rationale for selecting the feature does not apply.

ISSUE: SELECT OPTIONAL FEATURE: GET-TYPE POLLING MESSAGE

Description: The issue concerns selection of PING-type polling message.
Raised at: Feature 4.3.1.2 (a.2)

Decision: Select feature

Rationale: GET-type polling is necessary to retrieve specified information from network devices that is stored in internal device variables. The information is used in many (though not all) Fault Health Index Computation functions to periodically compute a "health index" value. (See optional feature COMPUTE FAULT "HEALTH INDEX." (1) Network Management Architecture. The rationale for selecting this feature is similar to that described in the issue SELECT OPTIONAL FEATURE: COMPUTE FAULT "HEALTH INDEX." (2) Global Network Structural Characteristics. The additional traffic should not result in the degradation of overall network performance due to network size, bandwidth, and topology.

Determines: Specialization of Function **Form Polling Messages** into **Form GET-type Polling Messages for Consolidated Organization.**

Decision: Do not select feature

Rationale: The rationale for selecting the feature does not apply.

ISSUE: SELECT OPTIONAL FEATURE:
AUTOMATIC POLLING TIME INTERVAL CONTROL

Description: Selection of this feature allows use of Automatic Polling Time Interval (PTI) Adjustment Algorithm. Specifically, selection of this feature will allow the network administrator to set the rate at which the PTI may change.
Raised at: Feature 4.3.1.2 (b-2.2)

Decision: Select feature.

Rational: Staffing. Requirements for staffing a network operations center influence selection of this feature.
Determines: Selection of function **Determine Polling Time Interval** and data flow "Poll Response Statistics."

Decision: Do not select feature.

Rational: Lack of staffing constraints indicates that this feature should be omitted.

ISSUE: SELECT OPTIONAL FEATURE:
PARTITIONED POLLING TIME INTERVAL SCOPE

Description: Selection of this feature allows specification of whether a Polling Time Interval (PTI) can be set for individual network partitions (also referred to as management domains).
Raised at: Feature 4.3.1.2 (b-2.3)

Decision: Select feature.

Rational: This feature should be selected together with selection of the alternative feature **Partitioned Monitoring Organization.**
Determines: Specialization of function **Initiate Polling** into **Initiate Polling for Partitioned Organization**; if optional feature **Automatic Polling Time Interval Control** is selected, function **Maintain Partitioned Polling Response Statistics.**

Decision: Do not select feature.

Rational: Consolidated monitoring organization was selected.
Determines: Specialization of function **Initiate Polling** into **Initiate Polling for Consolidated Organization**; if optional feature **Automatic Polling Time Interval Control** is selected, function **Maintain Consolidated Polling Response Statistics.**

ISSUE: SELECT OPTIONAL FEATURE:
INDIVIDUAL POLLING TIME INTERVAL SCOPE

Description: Selection of this feature allows specification of a separate Polling Time Interval (PTI) for individual network devices.

Raised at: Feature 4.3.1.2 (b-2.3)

Decision: Select feature.

Rational: (1) Resource Criticality Rank: The existence of a small number of very high priority devices justifies the need to set separate polling time intervals for individual network resources. (2) Network Operating Modes: The existence of operating modes may also contribute to the need for finer-grained control over the polling of network resources.

Determines: Specialization of function **Initiate Polling** into **Initiate Polling for Individual Network Resources.**

Decision: Do not select feature.

Rational: A small number of very high priority devices does not exist.

ISSUE: SELECT OPTIONAL FEATURE:
SET ALARM THRESHOLDS

Description: Selection of this feature allows the network operator to remotely set or reset threshold levels for alarm notifications maintained by agent systems.

Raised at: Feature 4.3.1.3

Decision: Select feature.

Rational: (1) Network Operating Modes and Resource Criticality Rank. The existence of operating modes may require different threshold levels for different modes (as for instance higher or lower levels during war than in peace. (2) Staffing. Staffing constraints may require greater automation of the ability to manipulate threshold values maintained as variables on remote network resources. (3) Global Network Structural Characteristics. If a large number of network resource are to be

managed, the ability to remotely set alarm thresholds will save time and effort.

Determines: Parameterization of function **Control Alarm Thresholds**.

Decision: Do not select feature.

Rational: Network Operating Modes are not a factor in the context of the application system.

4.4.3 Issues and Decisions in Filtering

This section has the following issues:

- Select Optional Feature: Remote Filtering Location
- Select Optional Feature: Event Profile Set Control
- Select Alternative Feature: Event Profile-Partition Association
- Select Alternative Feature: Type of Event Profile-Partition Association

---

ISSUE: SELECT OPTIONAL FEATURE:
REMOTE FILTERING LOCATION

Description: Selection of this feature allows network administrator to locate filter within the device agent.

Raised at: Feature 4.3.2.1 (b)

Decision: Select feature.

Description: Use of automatic or semi-automatic commands to SET values of device variables is selected.

Rationale: (1) Management Protocol Used: The protocol must support the ability to encode and transmit commands to device agents that allow remote filters to be defined and controlled. (2) Global Network Structural Characteristics: The use of remote filters in device agents will lessen the amount of traffic on the network. The selection of this feature is desirable if it will be important to ensure that a degradation of overall performance of the communications network will not occur. Estimating the network performance will require taking into account network size (number of devices), bandwidth capacities, and network topology. (3) Network Operating Modes: The existence of

certain operating modes may require that filtering be conducted locally. The decision to conduct remote filtering in response to changes in mode is specific to the application and organization. (4) The use of remote filtering locations in device agents should be consistent with administrative policies for network management.

Determines: This is an architectural issue. Selection of this feature parameterizes the domain architecture, not the model.

Decision: Do not select feature.

Rational: The feature will be less useful if the application system being developed does not have context features relating to Management Protocol Used, performance concerns, and Network Operating Modes.

ISSUE: SELECT OPTIONAL FEATURE:
EVENT PROFILE SETS

Description: Selection of this feature allows network administrator to define sets of event profiles and to enable and disable the operation of these sets.

Raised at: Feature 4.3.2.2 (c)

Decision: Select feature.

Rationale: (1) Communications Network Operating Modes. The existence of operating modes requires that event profiles specific to different modes be organized into sets. (2) Network management architecture. A distributed hierarchial network management architecture may require use of event profile sets where particular sets are used for nodes at different levels. In addition, changes in network operating mode (i.e. from peace to war) may change to position of a particular node in the architecture; i.e., from leaf node to intermediate. This requires different event profile sets for different positions. (3) Variable Network Alterability. A network that can take on a finite number of different physical organization may require different event profile sets for each organization. (4) Resource Criticality Rank. The existence of subsets of network resources with different priority levels may also necessitate the use of event profile sets.

Determines: Specialization of function **Control Filtering Constructs** into **Control Event Profiles.**

Decision: Do not select feature.

Rational: The feature is likely to be less useful if operating modes are not a factor and if the architecture is centralized.

Determines: Specialization of function **Control Filtering Constructs** into **Control Event Profile Sets.**

ISSUE: SELECT OPTIONAL FEATURE:
EVENT PROFILE-PARTITION ASSOCIATION

Description: This feature determines whether or not filtering constructs (either event profiles or event profile sets as determined below) are to be attached to network partitions. The feature is needed to respond to operating modes.

Raised at: Feature 4.3.2.2 (d)

Decision: Select feature

Rationale: (1) Network Structure Alterability and Resource Characteristic Alterability. (2) Operating Modes: Filtering constructs (event profiles or event profile sets) will be attached to network partitions to allow uniform responses to changes network structure, network composition, or changes in operating modes. This feature is required by the selection of **Dynamic Surveillance Control.**

Determines: See choice of alternative feature below.

Decision: Do not select feature

Rationale: The context features cited above are not factors in the network.

ISSUE: SELECT ALTERNATIVE FEATURE: TYPE OF EVENT PROFILE-PARTITION ASSOCIATION

Description: This feature determines whether filtering constructs are to be attached to network partitions as individual event profiles or as sets. This determination depends on whether or not the Event Profile Sets feature has been selected.

Raised at: Feature 4.3.2.2 (d)

Decision: Individual Construct Partition Association

Rationale: Individual event profiles will be attached to network partitions. This alternative should be selected if Event Profile Sets have not been selected.

Determines: Role players in a role for **network partition** relationship.

Decision: Construct Set Partition Association

Rationale: Event profile sets will be attached to network partitions. This alternative should be selected if Event profile Sets have been selected.

Determines: Role players in a role for **network partition** relationship.

4.4.4 Issues in Analysis Features

This section describes the following issues:

- Select Optional Feature: Enable/Disable Event Profile Action
- Select Optional Feature: Analysis Construct Set Control
- Select Optional Feature: Analysis Construct Partition Association
- Select Alternative Feature: Type of Analysis Construct Partition Association
- Select Optional Feature: Compute Statistical Summary Report
- Select Optional Feature: Compute Fault "Health Index"
- Select Optional Feature: Compute Network Resource Availability Summary

---

ISSUE: SELECT OPTIONAL FEATURE:
ENABLE/DISABLE EVENT PROFILE ACTION

Description: Selection of this feature allows the definition of alarm disposition rules that specify enable and disable actions for particular event profiles.

Raised at: Feature 4.3.3.1 (b.5)

Decision: Select feature

Rationale: (1) Global Network Structural Characteristics: Selection of this feature is justified by the need to reduce the level of alarm reporting activity caused by a large number of redundant alarm notifications. In communications networks with large network size and bandwidth restrictions, this is a desirable feature.
(2) "Bursty" Traffic Mode: Sudden upsurges in traffic may require that alarm notifications be triggered. Such upsurges may be caused by large transfers of multimedia information. In these cases, disposition rules may need to enable event profiles to filter out redundant notifications.

Determines: Output flow Event Profile Updates, coming from function Determine Alarm Disposition and as a control to the function **Filter Events**.

Decision: Do not select feature

Rational: Requirements to reduce level of unnecessary alarm reporting activity do not exist.

ISSUE: SELECT OPTIONAL FEATURE:
ANALYSIS CONSTRUCT SET CONTROL

Description: Selection of this feature allows network administrator to define sets of rules and to enable and disable these sets. This includes polling analysis rules, correlation rules, and alarm disposition rules.

Raised at: Feature 4.3.3.2 (b)

Decision: Select feature.

Rationale: (1) Communications Network Operating Modes. The existence of operating modes requires that analysis rules specific to different modes be organized into sets. Individual sets can then be enabled and disabled according to the current mode. (2) Network management architecture. A distributed hierarchial network management architecture may require use of different analysis rules for network management stations at different levels. In addition, changes in mode; i.e., from peace to war, may change to position of a particular station in the architecture; i.e., from leaf node to intermediate. This requires different rule sets for different positions. (3) Variable Network Alterability. A network that can take on a finite number of different physical organization may require different analysis construct sets for each organization.

Determines: Specialization of function **Control Analysis Constructs** into **Control Analysis Construct Sets.**

Decision: Do not select feature.

Rationale: The feature is likely to be less useful if operating modes are not a factor and if the architecture is centralized.

ISSUE: SELECT OPTIONAL FEATURE:
ANALYSIS CONSTRUCT PARTITION ASSOCIATION

Description: This feature determines whether or not analysis constructs are to be attached to network partitions. The feature is needed to respond to operating modes.

Raised at: Feature 4.3.3.2 (c)

Decision: Select feature

Rationale: Analogous to **SELECT OPTIONAL FEATURE: EVENT PROFILE-PARTITION ASSOCIATION**

Decision: Do not select feature

Rationale: Analogy applies as above.

ISSUE: SELECT ALTERNATIVE FEATURE: TYPE OF ANALYSIS CONSTRUCT PARTITION ASSOCIATION

Description: This feature determines whether analysis constructs are to be attached to network partitions as individual constructs or as sets. This determination depends on whether or not Analysis Construct Sets have been selected.

Raised at: Feature 4.3.3.2 (c)

The selection of alternatives is analogous to **SELECT ALTERNATIVE FEATURE: TYPE OF EVENT PROFILE-PARTITION ASSOCIATION**

ISSUE: SELECT OPTIONAL FEATURE: COMPUTE STATISTICAL SUMMARY REPORT

Description: Selection of this feature allows definition of statistical summary reports and control of the reporting. These include descriptions of the number of occurrences of particular kinds of event notifications on a set of the network resource over a specific time period.

Raised at: Feature 4.3.3.3 (a)

Decision: Select feature

Rationale: Network Management Architecture. An alarm surveillance system that is an "intermediate" or "leaf" node in a hierarchical distributed architecture may need to provide summary reports to a higher-level management station. Alarm surveillance systems in "peer to peer" architectures or centralized architectures may also require this feature.

Determines: Selection of function **Compute Statistical Summary**.

Decision: Do not select feature

Rationale: The alarm surveillance system is in a centralized network management architecture and therefore may not need this feature.

ISSUE: SELECT OPTIONAL FEATURE: COMPUTE FAULT "HEALTH INDEX"

Description: Selection of this feature allows network administrator to define a health index function to assess the status of the network with respect to faults.

Raised at: Feature 4.3.3.3 (b)

Decision: Select feature

Rationale: (1) Network Management Architecture. An alarm surveillance system that is an "intermediate" or "leaf" node in a hierarchical distributed architecture may need to compute a fault health index to provide an indicator of its overall status to a higher-level management station. Alarm surveillance systems in "peer to peer" architectures or centralized architectures will have less need. (2) Global Network Structural Characteristics. In cases where statistical computation functions are used, the additional traffic should not result in the degradation of overall network performance due to network size, bandwidth, and topology. (See rationale for issue **Select Alternative Feature: Define Polling Message Type.**)

Determines: Selection of function **Compute "Health Index" Value.**

Decision: Do not select feature

Rationale: The alarm surveillance system is in a centralized architecture or that is in a small distributed (hierarchical or "peer to peer") architecture may not need this feature.

ISSUE: SELECT OPTIONAL FEATURE: COMPUTE NETWORK RESOURCE AVAILABILITY SUMMARY

Description: Selection of this feature allows network administrator to define a reporting capability to summarize network resources that are available or "down."

Raised at: Feature 4.3.3.3 (c)

Decision: Select feature

Rationale: (1) Network Management Architecture. An alarm surveillance system that is an "intermediate" or "leaf" node in a hierarchical

distributed architecture may need to compute a summary of available and "down" resources to provide to a higher-level management station. Alarm surveillance systems in "peer to peer" architectures or centralized architectures will have less need. (2) Resource Criticality Rank. The status of network resources performing high-priority tasks need to be summarized to a higher-level management station or network administrator.

Determines: Selection of function **Compute Network Resource Availability Summary** (currently not provided in functional model).

Decision: Do not select feature

Rationale: The alarm surveillance system is in a centralized architecture or that is in a small distributed (hierarchical or "peer to peer") architecture may not need this feature.

4.4.5 Issues in Dynamic Control

This section describes the following issues:

- o Select Optional Feature: Scheduling
- o Select Optional Feature: Dynamic Mode Change Response

ISSUE: SELECT OPTIONAL FEATURE: SCHEDULING

Description: Selection of this feature allows network administrator to schedule automatic transitions of the operation of alarm surveillance operation, including changes in monitoring scope, monitoring strategy, and in the rules used to do filtering and analysis. These changes may be scheduled to meet the requirements of an "after hours" or "lights out" policy.

Raised at: Feature 4.3.4.1

Decision: Select feature

Rationale: (1) Daily Operating Modes: The existence of "after hours" and "lights out" policies and other planned scheduled transitions in daily operation of the network necessitates this feature. (2) Staffing Requirements. (3) Network Size: Staffing limitations may require automating scheduled changes in certain operations.

Determines: Selection of Function **Control Schedule Operation**.

Decision: Do not select feature

Rationale: Daily operating modes are not a factor. Staffing is adequate to control alarm surveillance manually.

ISSUE: SELECT OPTIONAL FEATURE: DYNAMIC MODE CHANGE RESPONSE

Description: Selection of this feature allows network administrator to program automatic responses to changes in network military modes, contingency modes, and reconstitution modes.

Raised at: Feature B.4.3.4.2

Decision: Select feature

Rationale: Contingency Modes. (1) Anticipated contingencies include the need to monitor a portion of the network normally outside the scope of an alarm surveillance system. The ability to program an automatic set of changes to occur in the event of such a contingency aids the network administrator in responding to the situation. (2) Military Modes and (3) Reconstitution Modes: Anticipated changes in military mode and reconstruction mode may involve changes in the scope of responsibility for individual managers and changes in monitoring strategy. (4) Resource Criticality Rank: In addition, the use of a different monitoring organization may be required that reflects a different prioritization of network resources in receiving monitoring services. The ability to program an automatic set of changes to occur in the event of changes in military modes aids the network administrator in responding to the situation. (5) Network Structure Alterability and (6) Resource Characteristic Alterability: Networks whose configuration can suddenly change or in which network resources can suddenly be added or removed may need programmed change responses.

Determines: Selection of function **Control Mode Changes**.

Decision: Do not select feature

Rationale: Contingency situations will not be a factor in the network.

5. THE FUNCTIONAL MODEL

An overview of the Functional Model was provided in section 3.3. This section describes the components of the Functional Model in greater detail. The overall behavior of systems in the alarm surveillance domain is represented by model components that describe the functional decomposition of the domain, the data transformation performed by specific functions, and state transitions associated with specific functions. The model components focus on identifying both commonalities and differences in alarm surveillance functions. In particular, they show how the Functional Model is parameterized to produce functional requirements for specific alarm surveillance application systems.

5.1 Decomposition Overview

This section provides a hierarchical view of a generic decomposition of the alarm surveillance function as defined in section 2.1. Sections describing decomposition on non-leaf activities are shown in parenthesis. Activities that are specialized are shown with asterisks. Optional activities are indicated with a "+" superscript.

A0 Alarm Surveillance: Manager Function (Context Level) (sec. 5.2.2)
- A1 Process Incoming Transmissions*
- A2 Perform Surveillance Function (sec. 5.2.3.1)
  - A21 Control Surveillance Constructs (sec. 5.2.4.1)
    - A211 Coordinate Construct Control Operation*
    - A212 Control Filtering Constructs*
    - A213 Control Analysis Constructs*
    - A214 Control Network Partitions*
    - A215 Control Alarm Thresholds+
  - A22 Enforce Scope of Responsibility*
  - A23 Analyze Events (sec. 5.2.4.2)
    - A231 Analyze Poll Responses (sec. 5.2.5.1)
      - A2311 Compare Responses
      - A2312 Apply Polling Analysis Rules
      - A2313 Accumulate Poll Response Statistics*
    - A232 Filter Events
    - A233 Correlate Events (sec. 5.2.5.2)
      - A2331 Apply Correlation Rules
      - A2332 Form Log Inquiries
      - A2333 Maintain Active Correlation Data
    - A234 Determine Alarm Disposition
    - A235 Identify Alarm Destinations
  - A24 Compute Summary Report+*
- A3 Poll Agents (sec. 5.2.3.2)
  - A31 Determine Polling Time Interval
  - A32 Form Polling Messages*
  - A33 Initiate Polling*
- A4 Process Outgoing Messages*

Within this decomposition, **Perform Surveillance Function** provides the capabilities described by the **Monitoring Scope**, **Filtering**, **Analysis**, and **Dynamic Surveillance Control** operational features. **Poll Agents** provides the capabilities of the **Polling Control** feature. The elaboration of this hierarchy and description of activities is provided in the next section. The overview provides a roadmap by which to understand the ensuing discussion.

5.2 Data Transformations and Controls

This section describes the functions shown in the decomposition overview above, including the explanation of the function performed, the input flow of data, the output flow, and the controls on the function. In the ensuing subsections, each level shown in the decomposition above is elaborated in detail. Appendix B.1 describes the correspondence between individual data and control flows and the entity and relationship definitions in the Information Model that describe the flows in more detail. Appendix B.2 describes what activities create, read, update, and delete particular entities and relationships.

At each level, information about commonalities and differences in functions is provided. The parameterizations called for by selections of operational feature and by direct consideration of context features are explicitly shown.

5.2.1 Notation Used

The representation chosen to depict data transformations and controls is IDEF0. An IDEF diagram consists of a set of functions--called *activities* in IDEF--that are linked by data and control flows. In keeping with the IDEF convention, the term activity will be used to describe individual functions. IDEF prescribes four types of flows for an activity, shown in figure 5.1. These are: Input Data Flows, Output Data Flows, Controls, and Mechanisms.

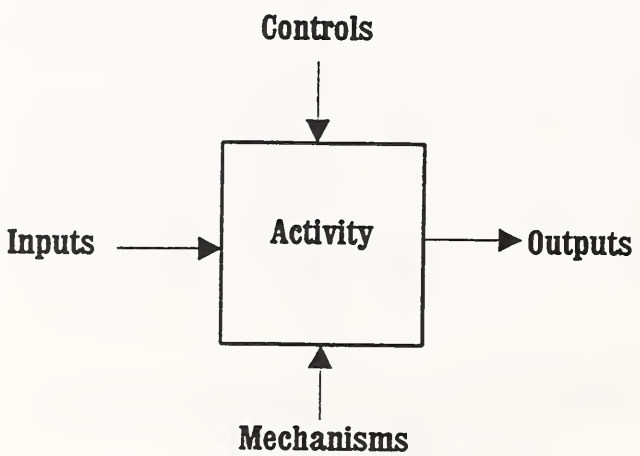


Figure 5.1: An IDEF0 Activity

Each IDEF diagram is accompanied by explanatory text that describes the activity in detail. All flows are explicitly listed. A glossary of terms in which each flow is defined is provided. The entries in the glossary contain references to the entity relationship model that contains more detailed descriptions of particular data and control flows.

IDEF diagrams are organized hierarchically to support the notion of functional decomposition. Individual functions--or activities--in higher-level diagrams are decomposed into a series of lower-level, more specific activities. In addition, inputs, outputs, controls, and mechanisms are also decomposed into more specific flows in the lower-level diagrams.

In IDEF, control flows represent data that regulate or constrain the production of outputs within an activity. Mechanisms are considered people, machines, resources, or existing systems that perform an activity or provide energy to an activity. Mechanisms are omitted in this version of the IDEF diagrams.

In this report, conventions for IDEF diagrams are altered to represent commonalities and differences among activities. Activities and flows that are parameterized by selection of operational features or directly parameterized by context features are indicated with the notation [active], indicating the name of the affecting feature. In addition, the accompanying explanatory text describes the parameterization.

5.2.2 First Level Decomposition: Alarm Surveillance

This decomposition describes the initial breakdown of the alarm surveillance function as shown in the context diagram. This function decomposes into four activities:

- A1 Process Incoming Transmissions
- A2 Perform Surveillance Functions
- A3 Poll Agents
- A4 Process Outgoing Messages

Activities A1 and A4, while outside the scope of alarm surveillance, are included in the domain model to provide the application developer with a more complete view (Some alarm surveillance systems may in fact be implemented as stand-alone systems). Activities A1 and A4 are specialized for specific management protocols. Activity A2 represents the core activities of alarm surveillance. Activity A2 provides the bulk of the capabilities described by the **Monitoring Scope**, **Filtering**, **Analysis**, and **Dynamic Control** operational features. Activity A3 is regarded by some as being outside the scope of alarm surveillance but is included in this study because it represents an essential aspect of monitoring communications networks. Activity A3 provides capabilities described by the **Polling** operational features. The decomposition of alarm surveillance is shown in figure 5.2a. The specialization of activities is shown in figure 5.2b.

EXPLANATORY TEXT:

A1 Process Incoming Transmissions (Event Notifications)

Description: This activity receives **Messages** from agent systems in specific network management protocols. The activity provides authorization and authentication services, parses the message and extracts event information ("user data") using **Message Translation Rules**, including Binary Encoding Rules and other rules described in the activities' decomposition in Appendix C, and formats and categorizes the event information for subsequent filtering and analysis activity. All event notifications are sent to an event log as **Log Updates**.

Input: Messages containing event notifications in a specific management protocol format.
Output: Event Notifications and Log Updates formatted for transmission.
Control: Message Translation Rules
Parameterization: None

Specialization: Activity A1 is specialized in two ways:

(1) As activity A1a **Process Incoming SNMP Transmissions**, which performs authentication, authorization, decoding, and formatting of SNMP **Messages**.

(2) As activity A1b **Process Incoming CMIP Transmissions**, which decodes and formats CMIP **Messages**.

The specializations are shown graphically in figure 5.2b. Their decomposition is described in Appendices C.1 and C.2.

A2 Perform Surveillance Functions

This activity controls the definition of the scope of the alarm surveillance system and carries out filtering and analysis functions.

Description: The activity enforces the scope of responsibility of an alarm surveillance system--ensuring that only those **Event Notifications** are processed that fall within the management domain of a particular alarm surveillance system. Event Notifications that are within the scope of the alarm surveillance system are filtered and correlated to identify alarms that pertain to faults effecting the communications network. Filtering and analysis are performed using filtering and analysis constructs, which are specializations of **Surveillance Constructs**. (These are described in more detail in subsequent decompositions of this activity). The operation of these constructs is controlled using **Construct Operation Control**. To correlate Event Notifications, information is retrieved from event logs; **Network Configuration** information, including connectivity and containment relationships between resources, is retrieved from network configuration databases. After correlation, other analysis constructs may be used to determine one of several actions that may be taken on alarm notifications. Alarm notifications may be reported as alarms to predetermined destinations (**reported alarms**) within the network. **Follow-Up Manager Inquiries** are sent to obtain more information from agents for network resources.

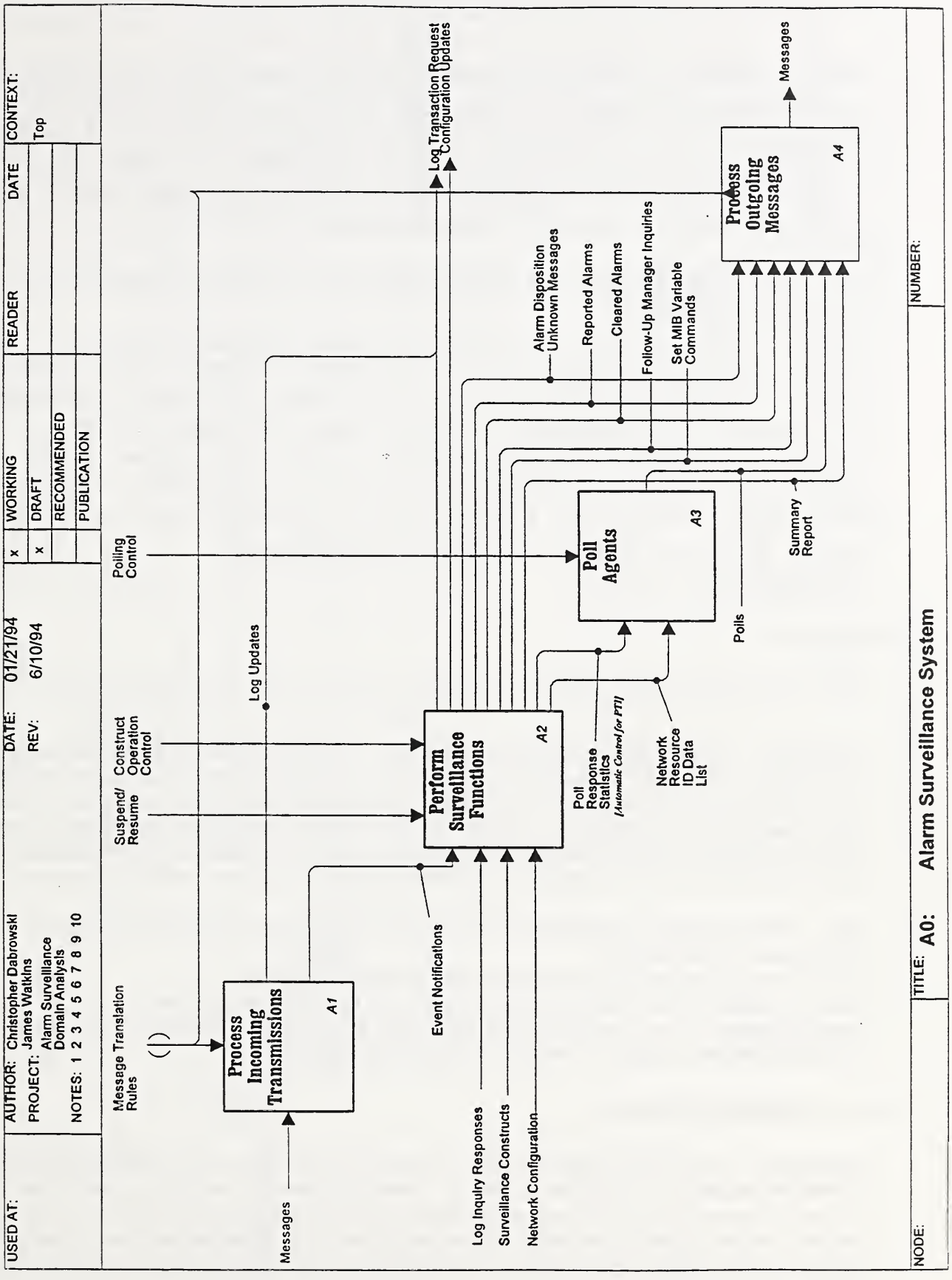


Figure 5.2a: Decomposition of Alarm Surveillance (Manager)

Alarm notifications for which the associated fault conditions have been corrected may be cleared (**Cleared Alarms**). In cases where the alarm surveillance system does not know how to handle the notification, an **"Alarm Disposition Unknown" Message** is sent. Records of these actions are recorded as **Log Updates** in a system log. Poll Responses (a subtype of Event Notifications) are tabulated to provide **Poll Response Statistics** needed by Activity A3. See decomposition of Activity A3.

Input: Event Notifications, Log Inquiry Responses, Surveillance Constructs, and Network Configuration.
Output: Reported Alarms, Cleared Alarms, "Alarm Disposition Unknown" Messages, Follow-Up Manager Inquiries, Configuration Updates, Log Transaction Requests (including log inquiries and updates), Poll Response Statistics (parameterized by the optional feature **Automatic Control of Polling Time Interval**), Set Management Information Base (MIB) Variable Commands (See glossary and [DABR93] for a definition of MIBs; see this activities' decomposition for more information on this data flow), Network Resource Identification Data List.
Control: Construct Operation Control and Suspend/Resume.
Parameterization: None

A3 Poll Agents

This activity sends poll messages to agents responsible for network resources.

Description: Two types of poll messages may be sent. **PING-Type Polls** check if the device is "up" or operating. **GET-Type Polls** retrieve information from variables that can be interpreted to provide more detailed status information used in calculations such as the "health index" computation, described in the decomposition of Activity A2. The activity may maintain one or more lists of network resources to be polled together with their addresses. Polls may be sent: (1) automatically at predetermined polling time intervals or (2) in response to a manual request made by the network administrator.

Input: Network Resource Identification Data List(s) and Poll Response Statistics (described in the decomposition of this activity).
Output: Polls (including both PING-Type Polls and GET-Type Polls).
Control: Polling Control controls polling operation and the polling time interval.
Parameterization: The input **Poll Response Statistics** is parameterized internally by the selection of the optional feature **Automatic Control of Polling Time Interval.**

A4. Process Outgoing Messages

Description: This activity provides protocol conversion services for outgoing **Messages** that transmit information originating in Activities A2 and A3. Inputs are converted into the appropriate management protocol for transmission to the agent systems using application layer management protocol interface services. Outgoing Messages are handed to the next lowest layer within the particular protocol (the transport layer in Internet protocol suite or the presentation layer in Open Systems Interconnection (OSI) suite).

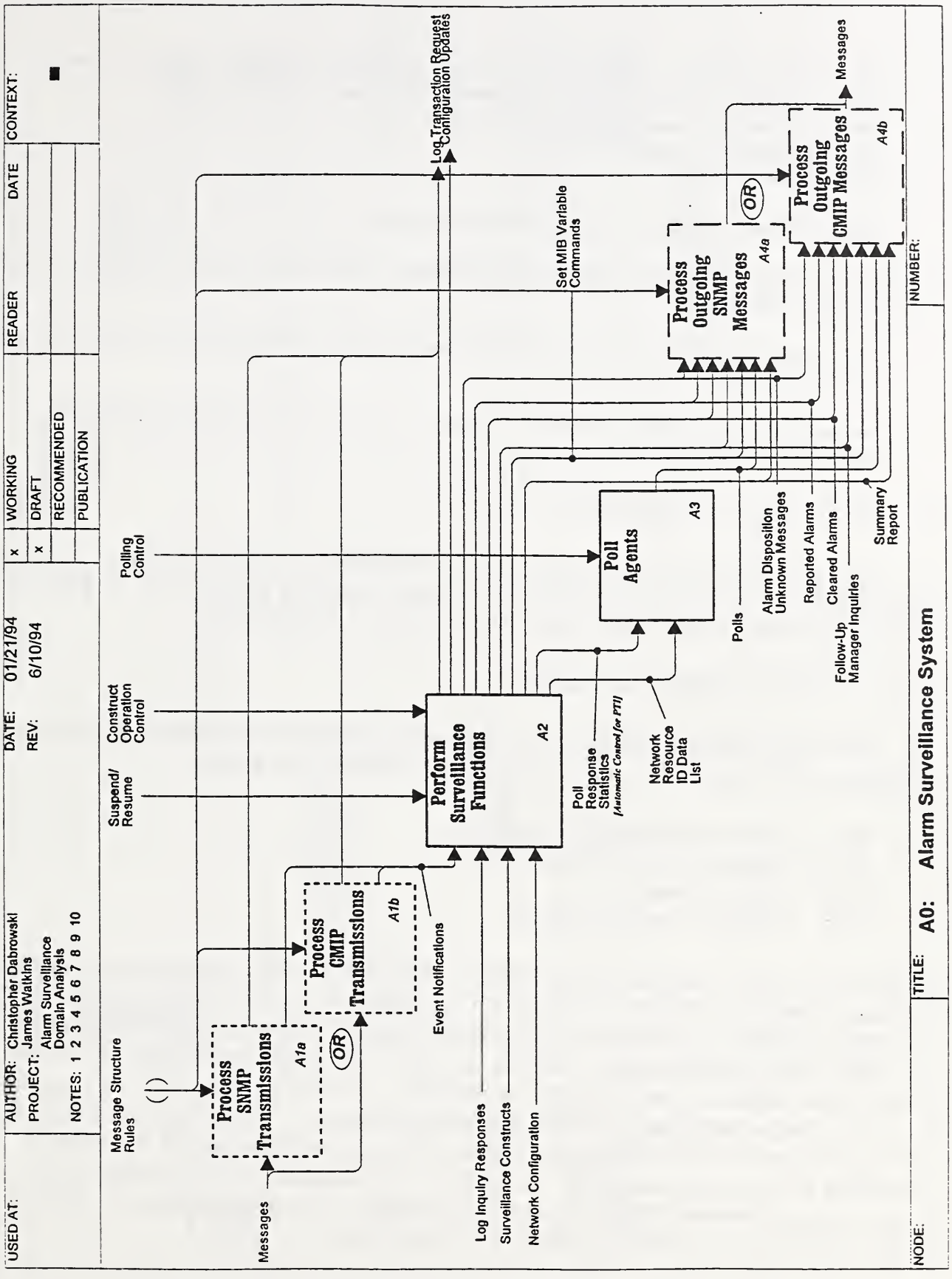


Figure 5.2b: Decomposition of Alarm Surveillance (specialized)

Input: Reported Alarms, Cleared Alarms, "Alarm Disposition Unknown" Messages, Follow-Up Manager Inquiries, SET MIB Variable Commands, Polls, and Summary Reports.
Output: Messages in management protocol format.
Control: Message Translation Rules
Parameterization: None

Specializations: Activity A4 is specialized in two ways:

(1) As activity A4a **Process Outgoing SNMP Messages** which provides protocol conversion services for SNMP messages.

(2) As activity A4b **Process Incoming CMIP Messages** which provides protocol conversion services for CMIP messages.

The specializations are shown graphically in figure 5.2b. Their decomposition is described in Appendices C.3 and C.4.

5.2.3 Second-Level Decompositions

This section describes two second-level decompositions. These include decompositions of Activity A2 **Perform Surveillance Function** and Activity A3 **Poll Agents**. The decompositions of activities A1 and A4 are found in Appendix C.

5.2.3.1 Perform Surveillance Function

This decomposition describes the breakdown of Perform Surveillance Function, shown as Activity A2 in figure 5.2a. Four more specific activities are shown:

- o A21 Control Surveillance Constructs
- o A22 Enforce Scope of Responsibility
- o A23 Analyze Events
- o A24 Compute Summary Report

Activities A21, A22, and A23 are mandatory. They provide the capabilities specified by operational features as follows. Activity A21 provides the capability to control alarm surveillance activities described by the operational features **Filtering Operation Control** and **(Analysis) Construct Operation Control**. Activity A21 is also specializable to provide **Dynamic Surveillance Control** feature capabilities. Activity A22 provides the capabilities of the feature **Scope Definition and Enforcement Mechanism**. The component activities of Activity A23 provide the filtering capabilities of the feature **Filtering** and the analysis capabilities of the feature **Analysis**. Activity A24 is parameterized by selection of the optional feature **Network Status Summary Reporting**. The decomposition of Activity A2 and its specialization are shown in figures 5.3a and 5.3b.

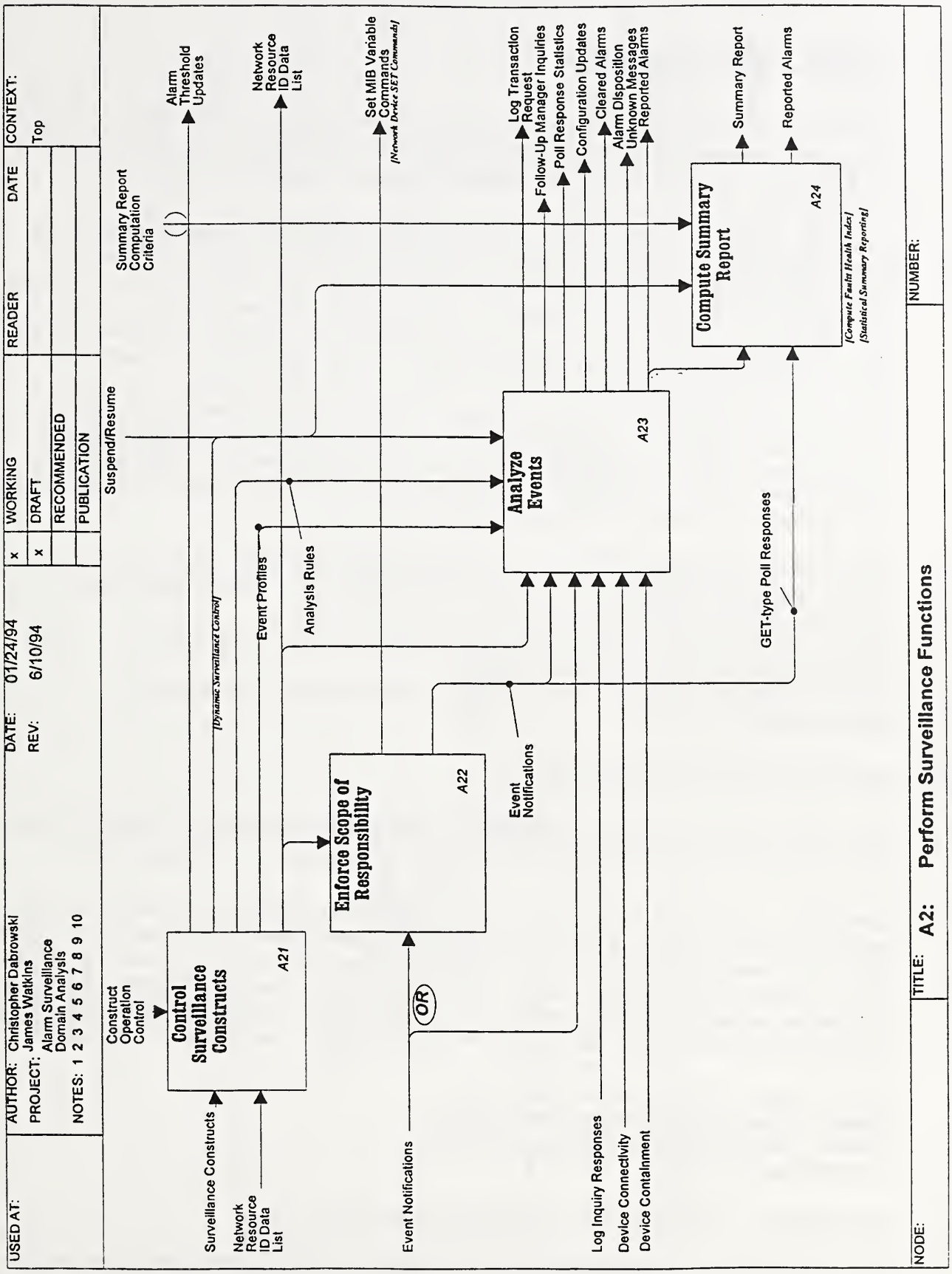


Figure 5.3a: Decomposition of Perform Surveillance Functions

A21 Control Surveillance Constructs

The activity controls the operation of constructs that in turn control the operation of the scope of responsibility enforcement function (Activity A21), the polling function (Activity A2), and the filtering and analysis functions (Activity A22).

Description: The activity takes as input from the network administrator or other external sources requests to add, delete, modify, and replace Surveillance Constructs. These constructs include (1) **Network Resource Identification Data List** and (2) **Surveillance Constructs**, consisting of filtering constructs, analysis constructs, network partition construct relationships and schedule constructs. (The last two inputs are described in the decomposition of this activity). **Construct Operation Control** is a control flow originating with the network administrator or other external source that enables or disables of the operation of network partitions, filtering constructs, and analysis constructs. The enable or disable commands result in the output of (1) specific **Network Resource Identification Data Lists** (corresponding to individual network partitions) that control **Enforce Scope of Responsibility**, activity A22, and serve as input to **Poll Agents**, Activity A2; (2) **Event Profiles** and **Analysis Rules** that provide control to activities within activity A23, **Analyze Events**; and (3) **Suspend/Resume** commands that turn filtering and analysis activity on and off.

Input: Network Resource Identification Data List (for network partitions), Surveillance Constructs (Filtering Constructs, Analysis Constructs, Network Partition construct relationships, Schedule constructs), and Alarm Threshold SET Request.
Output: Network Resource Identification Data Lists, Event Profiles, Analysis Rules, Suspend/Resume, and Alarm Threshold Update.
Control: **Construct Operation Control** to enable and disable Surveillance Constructs.
Parameterization: None

A22 Enforce Scope of Responsibility

The activity ensures that only those Event Notifications are processed that originate from network devices falling within the scope of an alarm surveillance system.

Description: The activity defines and enforces the scope of responsibility of the alarm surveillance system for network resources in one or more **Network Resource Identification Data List**. These data lists serve as control mechanisms that define the scope of responsibility. The method by which the scope of responsibility is enforced varies. This function can be carried out by (1) filtering Event Notifications on the basis of device address or (2) configuring network devices to transmit messages to the alarm surveillance system. The alternatives represent different specializations of this activity.

Input: Depends on specialization of this activity.
Output: Depends on specialization of this activity.
Control: Network Resource Identification Data List.
Parameterization: None

Specializations: This activity may be specialized in two ways:

(1) As activity A22a, **Control Network Device Configuration**, which defines and enforces the scope of responsibility by issuing SET commands to network devices it will control. These SET commands change the value of variables that determine where the device's agent sends its Event Notifications.

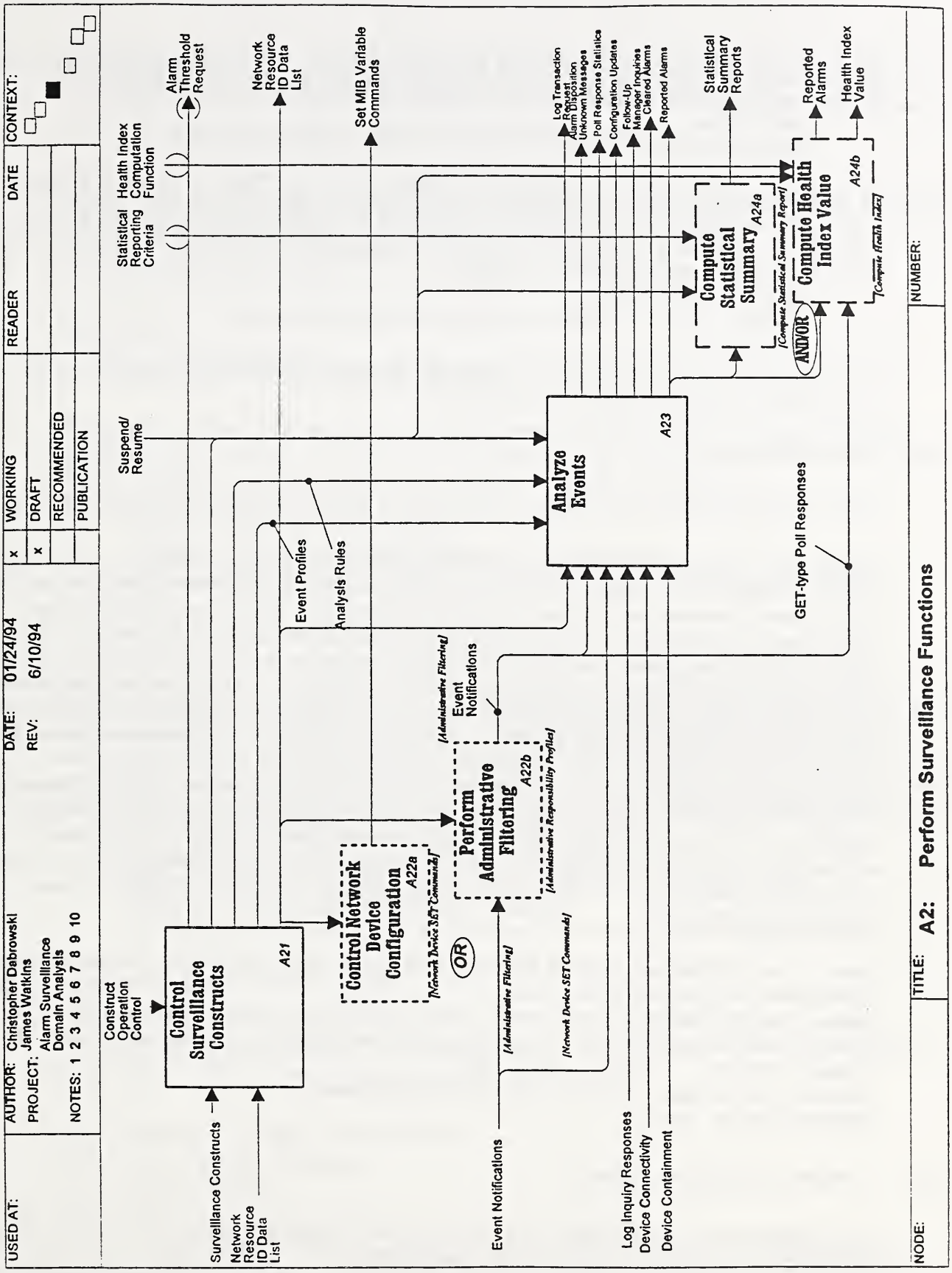


Figure 5.3b: Decomposition of Perform Surveillance Function (specialized)

The activity produces the output, **SET MIB Variable Commands**. This specialization is parameterized by the selection of the **Network Device SET Commands** alternative operational feature.

Input: None
Output: SET MIB Variable Commands (to change device configuration).

(2) As activity A22b, **Perform Administrative Filtering**, which uses filtering constructs to enforce the scope of responsibility. This specialization is determined by the selection of the **Administrative Responsibility Profiles** alternative operational feature. The activity takes Event Notifications as input and emits filtered Event Notifications as output.

Input: Event Notifications
Output: Event Notifications (including GET-type Poll Responses).

The control flow for both specializations is **Network Resource Identification Data Lists**. The specializations are shown graphically in figure 5.3b.

A23 Analyze Events

This activity performs the filtering and analysis functions of alarm surveillance.

Description: The activity receives **Event Notifications** (both solicited and unsolicited). Poll responses (a type of Solicited Event Notification) are compared against **Network Resource Identification Data Lists** to identify non-responding devices that may be experiencing faults. For Unsolicited Event Notifications, **event profiles** are used to filter out irrelevant or less important notifications. Once filtered, duplicate and related Event Notifications are correlated to more closely identify actual alarms that describe critical faults. Correlation requires use of information about the network configuration (**Device Connectivity** and **Device Containment**) as well as **Log Inquiry Results** describing historical information obtained through **Log Inquiries**. The activity determines the disposition of filtered and correlated alarm notifications--that is, determines what actions to take on them. This includes determining what destinations to send **Reported Alarms, Cleared Alarms,** and **"Alarm Disposition Unknown" Messages** (for alarms whose disposition cannot be determined). **Follow-Up Manager Inquiries** are sent when more information is required to determine the disposition of an alarm notification. **Configuration Updates** are issued to reflect effect of faults. **Analysis rules** are used to control poll response analysis, correlation, and determining alarm disposition. Details of these processes are given below.

Input: Event Notifications, Network Resource Identification Data Lists, Device Connectivity, Device Containment, and Log Inquiry Responses.
Output: Reported Alarms, Cleared Alarms, "Alarm Disposition Unknown" Messages, Follow-Up Manager Inquiries, Log Transaction Requests (inquiries and updates), Configuration Updates, and Poll Response Statistics.
Control: Event Profiles, Analysis Rules, and Suspend/Resume.
Parameterization: None

A24 Compute Summary Report

This optional activity computes summary reports describing the current status of a managed network with respect to detected faults.

Description: The activity may compute summary report information in one of two ways. Statistical summaries may be computed that describe number of occurrences of alarms of a particular kind within

a specified time interval. A "health index" value or values may be computed that summarize the overall state of the managed network. Two general variants are described as specializations. One or both computations may be selected as parameterized specializations of this activity. User-defined statistical criteria and computation algorithms control this activity.

Input: Reported Alarms and "GET-type" Poll Responses
Output: Summary Reports (including statistical summary report or "health index" values depending on how the activity is specialized) and Reported Alarm showing network status.
Control: Summary Report Computation Criteria and Suspend/Resume.
Parameterization: See specialization of this activity.

Specialization:

(1) As activity A24a **Compute Statistical Summary**

Description: The activity uses criteria defined by network administrators to compute summary statistics on the occurrence of particular event notifications over a defined time period. Both the type of event notification and the time interval are external controls for this activity.

Input: Reported Alarms
Output: Statistical Summary Reports
Control: Statistical Reporting Criteria and Suspend/Resume.
Parameterization: Selection of the **Statistical Summary Reporting** optional feature.

(2) As activity A24b **Compute "Health Index" Value**

Description: The activity applies a "health index" function to data in incoming event notifications to compute the summary "health index." A "health index" is a value that summarizes the overall state of the managed network. Typically, it is used to provide summary information about the network to a network administrator or a higher-level management station. The health index function contains a built-in threshold, which if exceeded, results in the generation of an alarm notification indicating the overall status of the network has declined. The specific function is highly variable and application dependent. If certain thresholds are exceeded, an alarm notification is emitted.

Input: Reported Alarms and "GET-type" Poll Responses.
Output: "Health Index" Value and Reported Alarm showing network status.
Control: "Health Index" Computation Function
Parameterization: Selection of the **Compute Fault "Health Index"** optional feature.

5.2.3.2 Decomposition of Poll Agents

This decomposition describes the breakdown of the Poll Agents, shown as Activity A3 in figure 5.2a. Three more specific activities are described:

- o A31 Determine Polling Time Interval
- o A32 Form Polling Messages
- o A33 Initiate Polling

Activity A33 is specialized to Activity A33a or A33b by the selection of **Consolidated** or **Partitioned** alternative features. The decomposition is shown in figure 5.4a. Specialization of activities is shown in figure 5.4b.

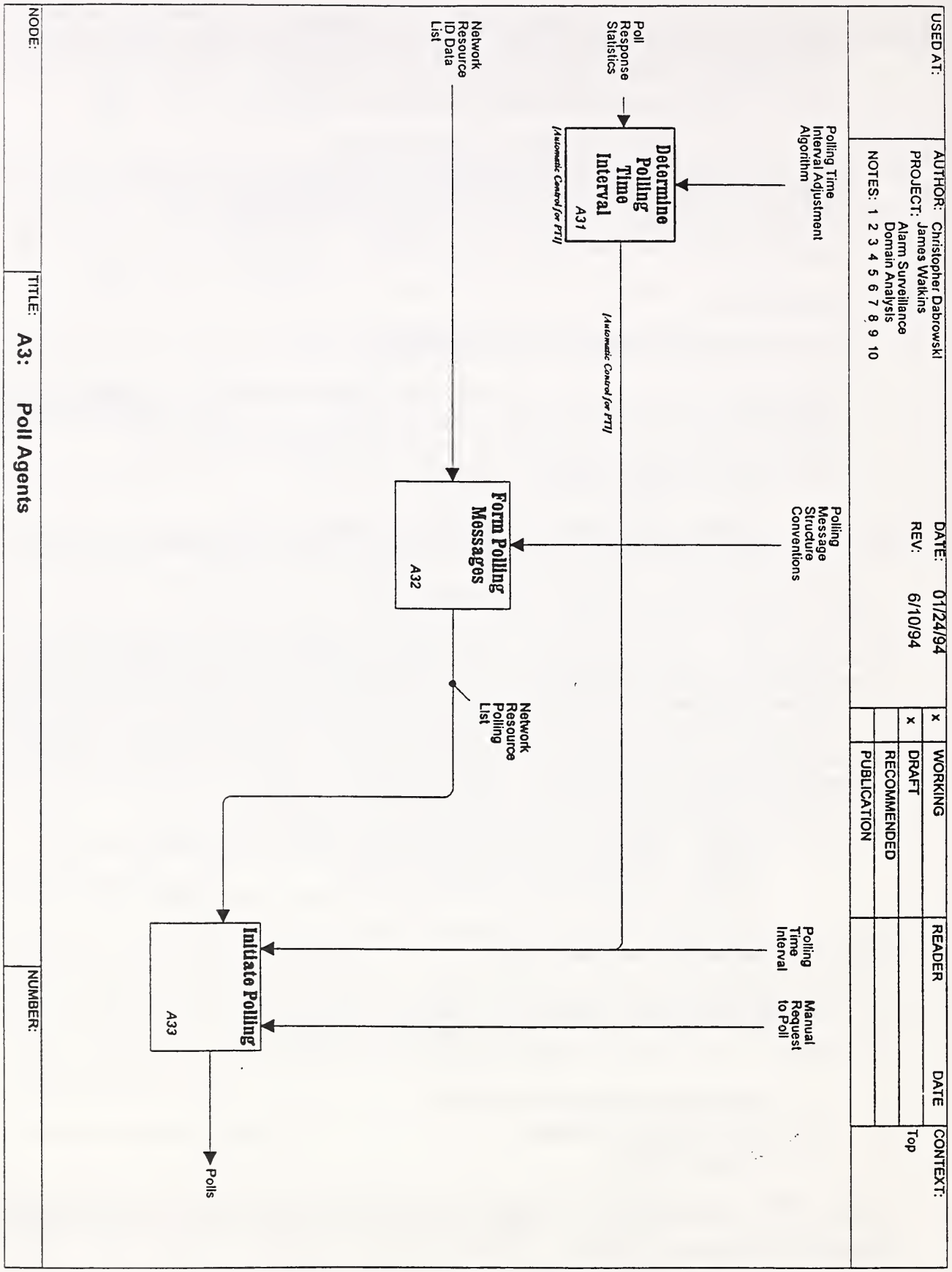


Figure 5.4a: Decomposition of Poll Agents

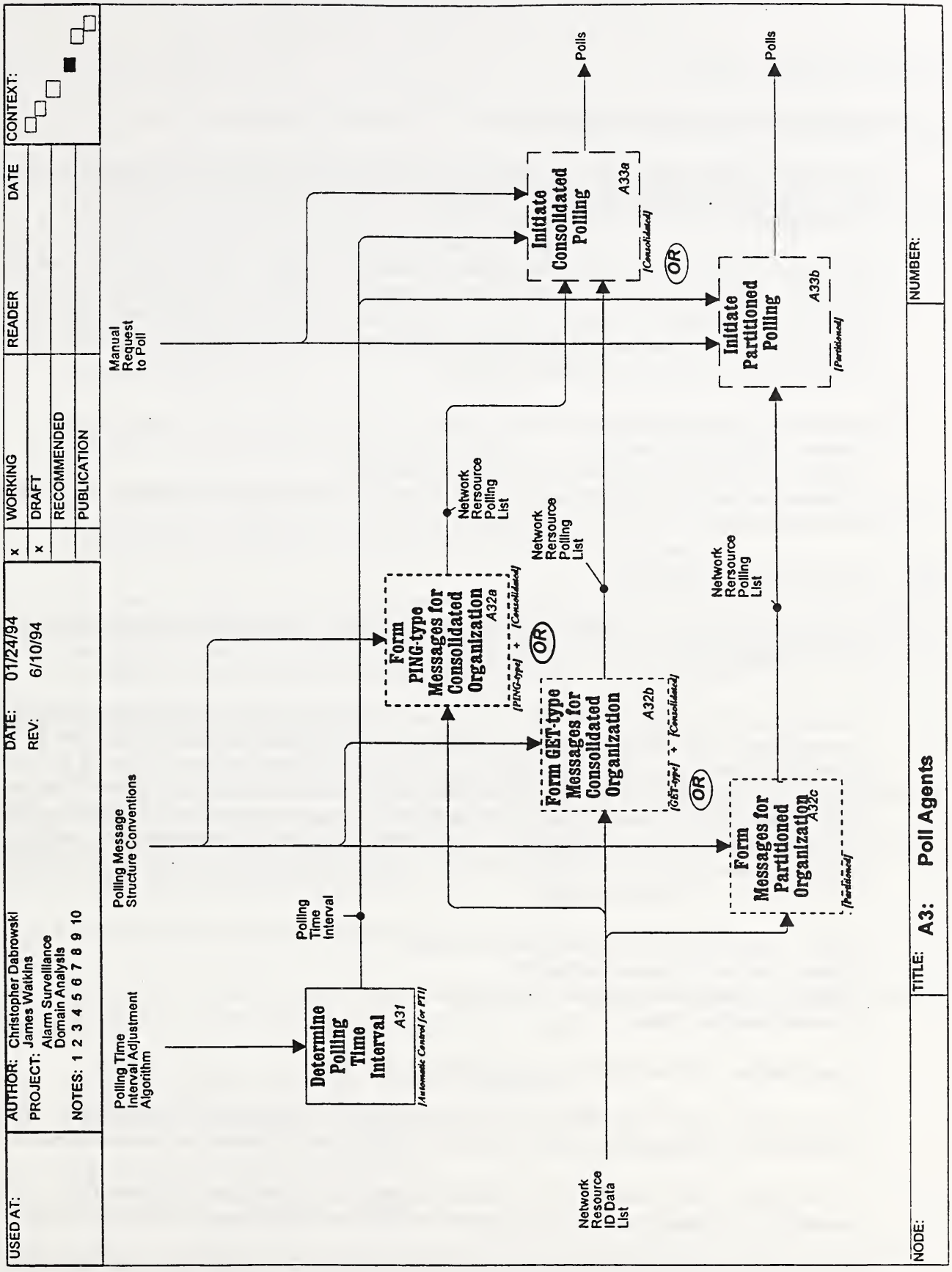


Figure 5.4b: Decomposition of Poll Agents (specialized)

EXPLANATORY TEXT

A31 Determine Polling Time Interval

This activity automatically determines the polling time interval (PTI), thus providing the capability of "self-adjusting" the PTI.

Description: The activity accepts **Poll Response Statistics** as input. These statistics are used by a polling time interval adjustment algorithm that calculates a new PTI. The calculation uses a comparison of responses to non-responses to determine how closely the network need to be monitored. This calculation is performed at specified time periods based on previously calculated PTIs. The results are sent to activity A33 **Initiate Polling.**

Input: Poll Response Statistics
Output: Polling Time Interval
Control: The Polling Time Interval Adjustment Algorithm
Parameterization: This activity is parameterized by the selection of the **Automatic Polling Time Interval Control** feature.

A32 Form Polling Messages

The activity forms individual polling messages for a set of devices and forwards them for transmission.

Description: The input to the activity is one or more **Network Resource Identification Data Lists,** corresponding to the relationship **Network Partition** (see Information Model), that includes all information necessary to form either PING-type or GET-type polling messages including device identification and device addresses. The activity may be specialized along two different lines: on the basis of type of polling message and on the basis of consolidated or partitioned organization. The output is **Network Resource Polling List,** a list of PING-type or GET-type **Polls** for an entire managed network in consolidated mode or for a particular network partition in partitioned mode. This output is sent to Activity A33, **Initiate Polling.**

Input: Network Resource Identification Data List
Output: Network Resource polling list
Control: Polling message structure conventions.
Parameterization: None

Specialization: The activity may be parameterized as follows:

(1) As activity A32a, **Form PING-type Polling Messages for Consolidated Organization.** This specialization is parameterized by the selection of **PING-type Poll Messages** alternative feature.

(2) As activity A32b, **Form GET-type Polling Messages for Consolidated Organization.** This specialization is parameterized by the selection of **GET-type Poll Messages** alternative feature.

(3) As activity A32c, **Form Polling Messages for Partitioned Organization,** on the basis of the selection of **Partitioned Network Organization** alternative feature. This activity allows formation of either **PING-type Poll Messages** or **GET-type Poll Messages** for individual partitions.

A33 **Initiate Polling**

This activity maintains information on polled network resources and initiates polls.

Description: The activity receives and maintains **Network Resource Polling List**, the output of Activity A32. The activity initiates transmission of these poll messages according to the polling time interval (PTI). The activity may be specialized to maintain a single list or multiple lists corresponding to single or multiple network partitions as described below.

Input: Network Resource Polling List
Output: Polls
Control: Polling Time Interval and Manual Request to Poll.
Parameterization: None

Specialization: The activity may be specialized in two ways, on the basis of selection of either consolidated or partitioned monitoring organization:

(1) As activity A33a, **Initiate Consolidated Organization Polling**. In this specialization, a single set of information on polled network resources is maintained. The specialization is parameterized by selection of the **Consolidated Monitoring Organization** optional feature.

(2) As activity A33b, **Initiate Partitioned Organization Polling**. In this specialization, multiple sets of information about polled resources corresponding to different network partitions are maintained. Each partition may be polled according to a different time interval. The specialization is parameterized by selection of the **Partitioned Monitoring Organization** optional feature.

5.2.4 Third Level Decompositions

This section provides third level decompositions for selected activities described in section 5.2.3. These include decompositions for Activity A21 **Control Surveillance Constructs** and Activity A23 **Analyze Events**. Third-level decompositions of other second-level activities was not deemed necessary.

5.2.4.1 Control Surveillance Constructs

This section describes the breakdown of **Control Surveillance Constructs**, Activity A21 in figure 5.3a. This decomposition, shown in figure 5.5a, consists of:

- A211 Coordinate Construct Control Operation
- A212 Control Filtering Constructs
- A213 Control Analysis Constructs
- A214 Control Network Partitions
- A215 Control Alarm Thresholds

Activity A211 is parameterized by the selection of the **Dynamic Surveillance Control** optional operational feature. Activity A215 is specialized by the selection of **Set Alarm Thresholds**. Specializations of activities are shown in figure 5.5b.

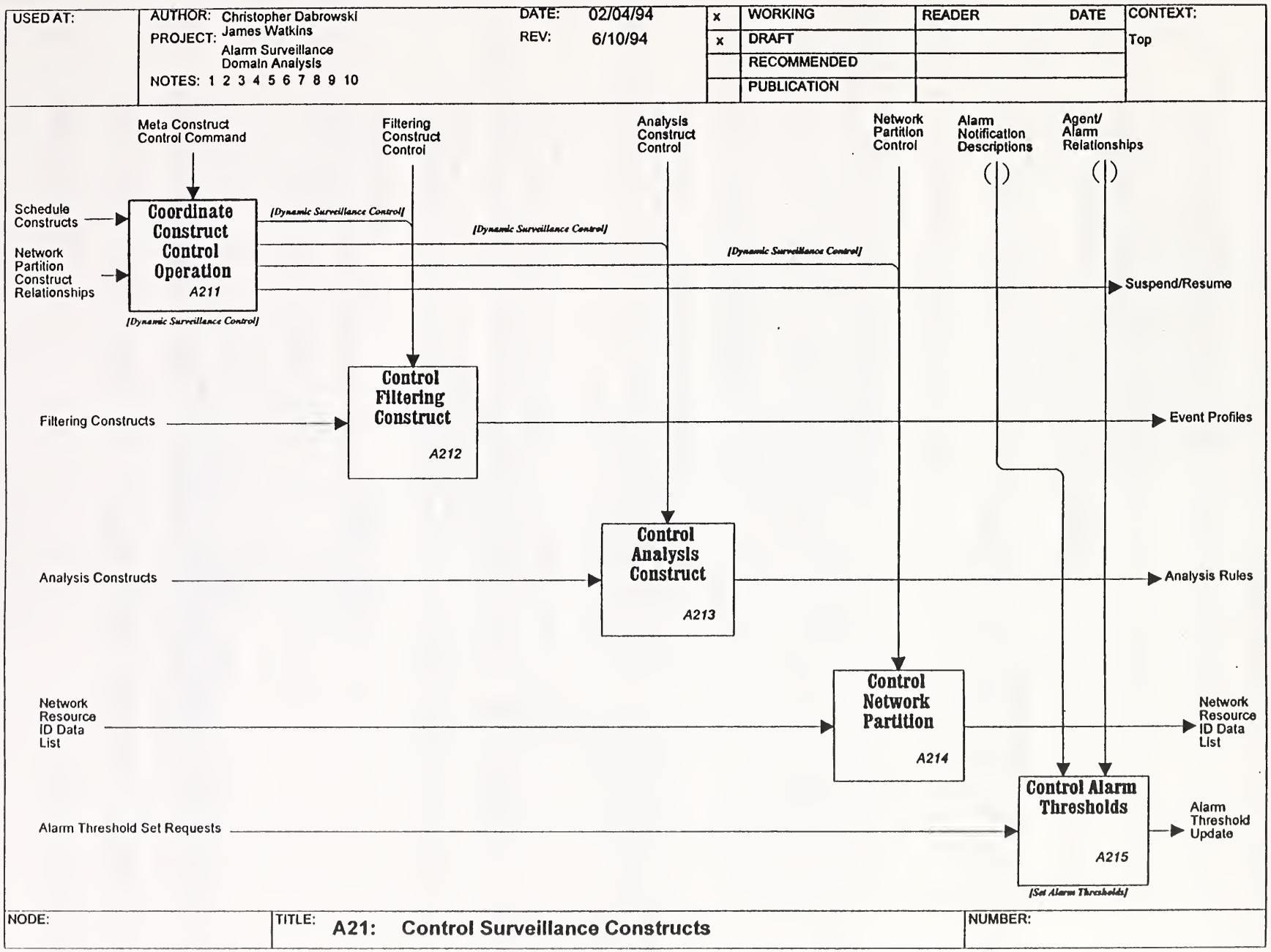


Figure 5.5a: Decomposition of Control Surveillance Constructs

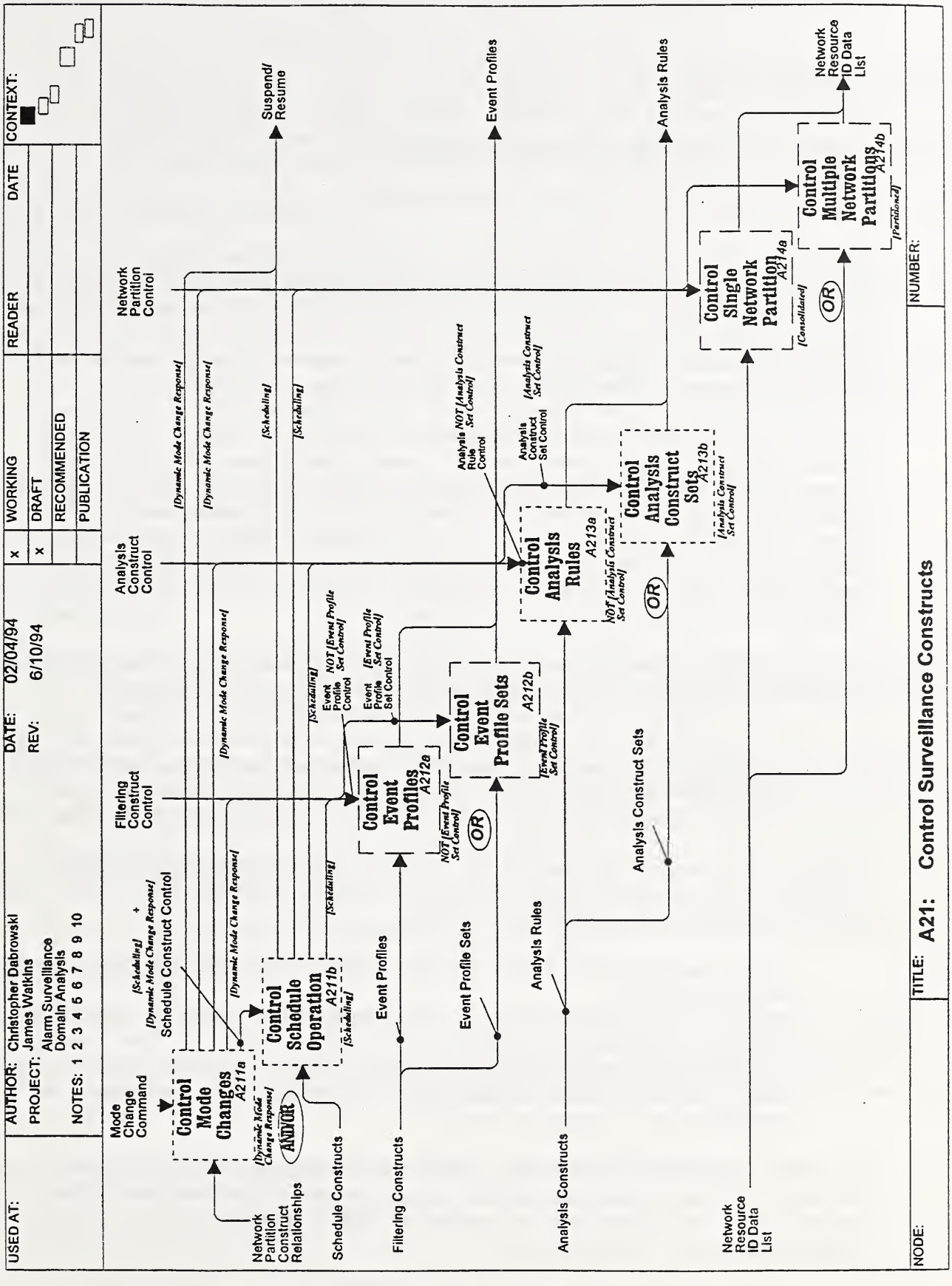


Figure 5.5b: Decomposition of Control Surveillance Constructs (specialized)

EXPLANATORY TEXT:

A211 Coordinate Construct Control Operation

This activity provides dynamic control capabilities.

Description: The activity provides the ability to dynamically coordinate changes in the operation of event profile sets, analysis rule construct sets, and network partitions to respond to changes in network operating modes. Specific event profile sets, analysis construct sets, and network partitions may be associated with particular operating modes. The operation of construct sets and network partitions that are related to a particular operating mode may be changed together (1) by commands issued by a network administrator or other external source or (2) according to a schedule.

Input: Network Partition Construct Relationships, and Schedule Constructs.
Output: Filtering Construct Control Commands, Analysis Rule Construct Control Commands, Network Partition Control Commands (representing enabling or disabling operations of particular resources), and Suspend/Resume activity commands to turn filtering and analysis on or off.
Control: Meta-construct control, specialized as described in activities A211a and A211b.
Parameterization: Selection of **Dynamic Surveillance Control** optional operational feature.
Specialization: The activity has two specializations. The selection of features may parameterize the selection of one or both of the specialized activities.

(1) A211a **Control Mode Changes.** The activity responds to **mode change** commands that indicate changes in operating mode. The activity emits specific enable and disable commands

- to activity A212b to control the operation of event profile sets (**Event Profile Set Control**).
- to activity A213b to control the operation of analysis rule construct sets (**Analysis Rule Construct Set Control**).
- to activity A214b to control the operation of network partitions (**network partition control**).

Specific sets and partitions are associated with particular modes. See the **Network Partition** relationship in the Information Model. This construct shows the relationship between event profile sets, analysis rule construct sets, and network partitions.

> **Input:** Network Partition Construct Relationships that relate specific operating modes to network partitions.
> **Output:** As in Activity A211 and also **Schedule Construct Control** (described in A211b).
> **Control:** Mode Change Command.
> **Parameterization:** Selection of **Dynamic Mode Change Response** optional operational feature. Schedule Construct Control output is also parameterized by selection of the **Scheduling** optional operational feature.

(2) A211b **Control Schedule Operation.** This activity controls the operation of schedule constructs. The activity implements particular schedules, issuing **Construct Control commands** called for at scheduled times. Its operation may be overridden by **Mode Change Commands.** See use of **Schedule** entity in the Information Model.

> **Input:** The input is specialized to receive Schedule Constructs and Network Partition Construct Control.
> **Output:** As in Activity A211.

Control: The activity is specialized to be controlled by **Scheduling Construct Control** that enables and disables schedule constructs. This control may be issued by the network administrator or by activity A211a.
Parameterization: Selection of **Scheduling** optional operational feature.

A212 Control Filtering Constructs

This activity performs update actions to, and controls the operation of, individual event profiles or event profile sets.

Description: The activity maintains filtering constructs (either individual event profiles or event profile sets). It accepts commands to update these constructs, including add, delete, and modify operations. In response to **Filtering Construct Control** commands, the activity determines what event profiles to provide to activity A23 **Analyze Events** for filtering purposes.

Input: Filtering Constructs and additions, updates, and deletions to Filtering Constructs.
Output: Event profiles
Control: Filtering Construct Control
Parameterization: None

Specialization:

(1) A212a **Control Event Profiles.** This activity controls Individual Event Profiles. It is controlled by Filtering Construct Control. This selection is parameterized by not selecting the **Event Profile Sets** optional feature. The input to this activity is specialized to **Event Profiles.**

(2) A212b **Control Event Profile Sets.** This activity controls Event Profile Sets. It is controlled by **Filtering Construct Control.** This selection is parameterized by selecting the **Event Profile Sets** optional feature. The input to this activity is **Event Profile Sets.**

A213 Control Analysis Constructs

This activity performs update operations to, and controls the operation of, analysis rules and analysis construct sets.

Description: The activity maintains analysis constructs (either individual analysis rules or analysis construct sets). It accepts commands to update these constructs, including add, delete, and modify operations. In response to **Analysis Construct Control** commands, the activity determines what analysis rules to provide to activity A23 **Analyze Events** to do polling analysis, correlation, and alarm disposition.

Input: Analysis Constructs and additions, updates, and deletions to Analysis Constructs.
Output: Analysis Rules
Control: Analysis Construct Control
Parameterization: None

Specialization:

(1) A213a **Control Analysis rules.** This activity controls Individual analysis rules. It is controlled by Analysis Rule Construct Control. This selection is parameterized by not selecting analysis construct organization. The input to this activity is specialized to **Analysis Rules.**

(2) A213b **Control Analysis Construct Sets.** This activity controls Analysis Rule Construct Sets. It is controlled by Analysis Rule Construct Set Control. This selection is parameterized by selecting analysis construct organization. The input to this activity is specialized to **Analysis Construct sets.**

A214 Control Network Partition

This activity performs update actions to, and controls the operation of, one or more network partitions.

Description: The activity maintains network partitions (either a single partition for the entire network in the consolidated mode, or multiple partitions in the partitioned mode). It accepts commands to update information on network resources for partitions, including add, delete, and modify operations. In response to **Network Partition Control** commands, **Network Resource Identification Data Lists** are sent to A23 **Analyze Events** (for polling analysis) and to activity A3 **Poll Agents.**

Input: Network Resource Identification Data List(s)
Output: Network Resource Identification Data List(s)
Control: Network partition control
Parameterization: None

Specialization:

(1) A214a **Control Single Network Partition.** This activity controls the device identification information for an alarm surveillance system in a single unit--one network partition. The activity is parameterized by the selection of **Consolidated Monitoring Organization.**

(2) A214b **Control Multiple Network Partitions.** This activity controls multiple network partitions. The activity is parameterized by the selection of **Partitioned Monitoring Organization.**

A215 Control Alarm Thresholds

In response to external requests, this activity initiates update actions to change the value of alarm thresholds for alarms sent by agent systems. The update actions are performed by the agent systems on their own internal data structures.

Description: The activity takes as input **Alarm Threshold Set Requests** to set or modify alarm thresholds on particular network resources or on a set of network resources emitting a particular type of alarm notification. The request is checked to ensure it is valid, using **Alarm Notification Descriptions** to control the checking activity. For valid requests, the activity transforms the request into a form that can transmitted to the agent system. The agent can then update its own internally-maintained data structures to comply with the external update request. For requests to change the threshold on a set of devices that emit a particular type of notification, the activity maintains data that describes what network resources emit particular types of alarm notifications (**Agent/Alarm Relationships**). The

output of this activity, **Alarm Threshold Update**, is sent to Activity A4 **Process Outgoing Messages** for transmission to those agents.

Input: Alarm Threshold Set Requests
Output: Alarm Threshold Update
Control: Alarm Notification Descriptions and Agent/Alarm Relationships.
Parameterization: **Set Alarm Thresholds** Optional Feature

5.2.4.2 Decomposition of Analyze Events

This decomposition describes the breakdown of the Analyze Events shown as Activity A23 in figure 5.3a. The decomposition, shown in figure 5.6, consists of:

- A231 Analyze Poll Responses
- A232 Filter Events
- A233 Correlate Events
- A234 Determine Alarm Disposition
- A235 Identify Alarm Destinations

These activities are not currently parameterized.

EXPLANATORY TEXT

A231 **Analyze Poll Responses**

The activity checks poll responses against list of network resources to identify those devices that are non-responding.

Description: The input to this activity is **Poll Responses (PING-Type, GET-Type, and Polled Alarm Notifications)**. The activity maintains the list of network devices being monitored. Incoming poll responses are compared against the list of devices and are recorded. An alarm notification may be issued if a certain number of null responses occur for a device over a predetermined time period. Polling analysis rules control this activity by specifying conditions for issuing an alarm notification including the number of null responses occurring over a time period (specified by a polling time interval), the type of network device, the device priority, and other factors. There are two outputs: (1) **Alarm Notifications** are forwarded to **Correlate Events** and (2) statistical summaries of the number of poll responses and non-responses that are forwarded as **Poll Response Statistics** to activity **A3 Poll Agents**. The activity is controlled by **Polling Analysis Rules** and **Suspend/Resume** commands that can turn the activity off and on.

Input: Poll Responses (PING-Type, GET-type, and Polled Alarm Notifications) and Network Resource Identification Data List.
Output: Alarm Notifications and Poll Response Statistics.
Control: Polling Analysis Rules, Suspend/Resume.
Parameterization: None

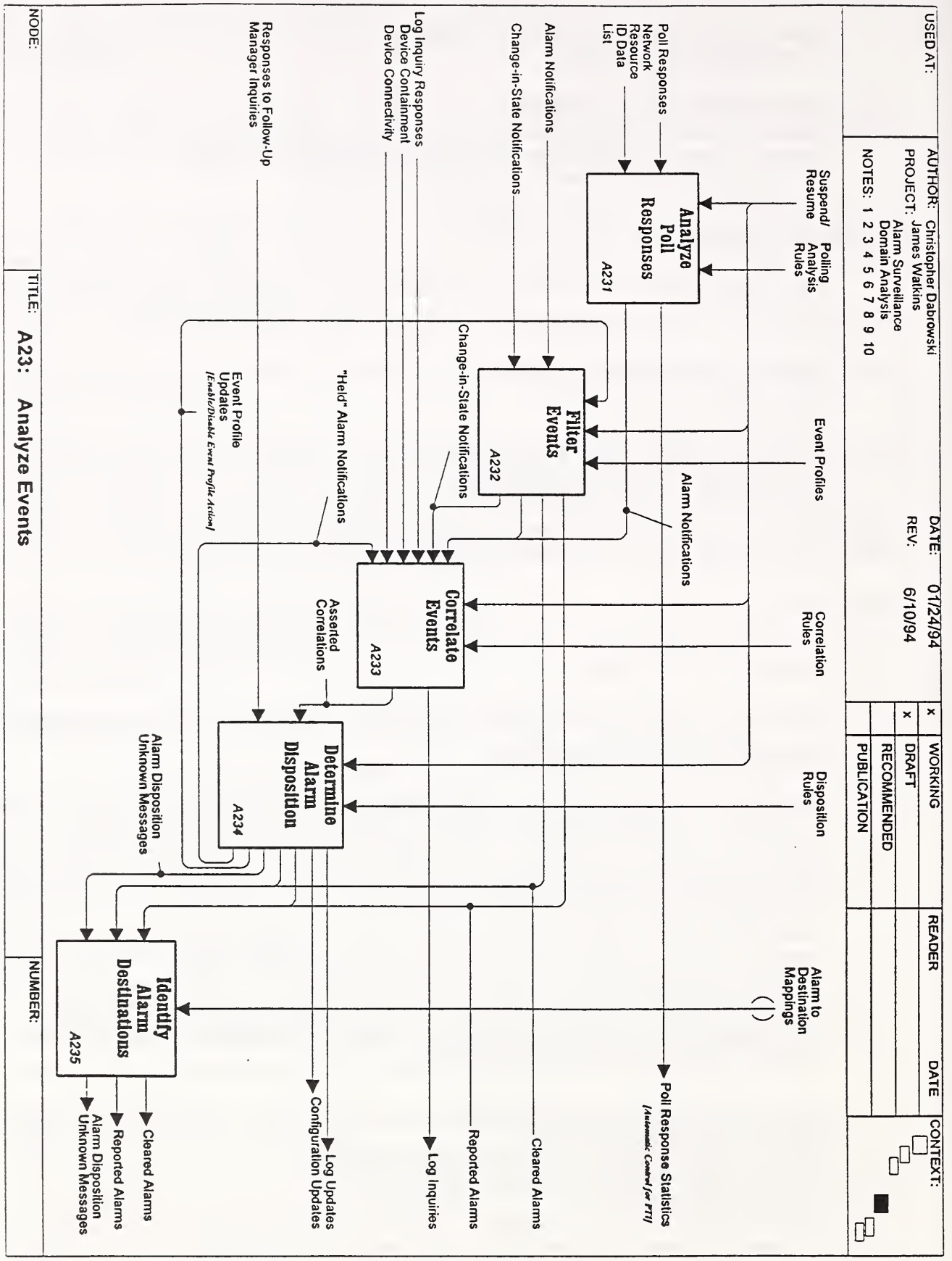


Figure 5.6: Decomposition of Analyze Events

A232 **Filter Events**

This activity filters Event Notifications to discard irrelevant Event Notifications and non-alarms.

Description: The activity takes as input **Unsolicited Event Notifications**. Incoming Event Notifications are compared against event profiles. Emergent alarms that require immediate attention are forwarded to the network administrator and other destinations as **Reported Alarms**. Alarms that have been cleared at their point of origin are forwarded to appropriate destinations as **Cleared Alarms**. Unsolicited Event Notifications (both alarm notification and change-in-state notifications) requiring further analysis are forwarded to **Correlate Events**. Control is provided by **Event Profiles** that specify what Event Notifications are to be filtered and **Suspend/Resume** that turns the activity off or on.

Input: Alarm Notifications and Change-in-State Notifications.
Output: Reported Alarms, Cleared Alarms, Alarm Notifications, and Change-in-State Notifications.
Control: Event Profiles, Event Profile Updates, and Suspend/Resume.
Parameterization: None

A233 **Correlate Events**

The activity correlates unsolicited Event Notifications (alarm notifications and change-in-state notifications) to identify notifications describing a single fault or a set of related faults.

Description: The activity correlates incoming alarm notifications, change-in-state notifications, and "held" alarm notifications that occur over a specified time interval to assert correlations that describe a single fault or a related set of faults. Correlations are asserted for related Event Notifications that may occur on the same or a connected set of network resources. The activity is controlled by **Correlation Rules** which are used to assert correlations and **Suspend/Resume** commands that turn the activity off and on. Asserted correlations are forwarded to **Determine Alarm Disposition** for action. Log inquiries may be made to retrieve logged Event Notifications for correlation with incoming notifications.

Input: (1) Alarm notifications, (2) Change-in-State Event Notifications, (3) Device Connectivity and Device Containment relationships between network resources involved in correlation operations; (4) Results of Log Inquiries, and (5) "Held" Alarm Notifications.
Output: Asserted Correlations and Log Inquiries.
Control: Correlation Rules and Suspend/Resume.
Parameterization: None

A234 **Determine Alarm Disposition**

This activity determines what actions to take on asserted correlations produced by activity A233.

Description: The activity takes the inputs **Asserted Correlations** and **Responses to Follow-Up Manager Inquiries**. The latter inputs contain additional information needed to make particular decisions. Using these inputs, the following decisions can be made:

(1) Reporting alarms resulting from correlations producing the output **Reported Alarms** which represents:

a. Collapsing correlated, multiple occurrences of an alarm into a single alarm.
b. Substituting a new alarm for a set of correlated alarm notifications.
c. Issuing a new alarm from a set of change-in-state Event Notifications.
d. Updating the status of a previously reported alarm--with a new severity level.

(2) Suppressing low-priority alarm in the presence of a correlated higher priority alarm.
(3) Suppressing further occurrences of a correlated alarm by updating event profiles (resulting in the output **Event Profile Updates**).
(4) Clearing alarms resulting from correlated change-in-state event reports (the output **Cleared Alarms**).
(5) Issuing data for **Follow-Up Manager Inquiries** requesting additional information from an agent system.
(6) Issuing **Configuration Updates**.

Rules used by this activity may also recognize situations for which specified actions have not been determined (such as certain partial correlations) and report them to a network administrator as **"Alarm Disposition Unknown" Messages.** The activity issues **Log Updates** describing dispositions taken. The activity is controlled by **Disposition Rules** which determine the decisions described above and **Suspend/Resume** commands that turn the activity off and on.

Input: Asserted Correlations and Responses to Follow-Up Manager Inquiries.
Output: Reported Alarms, Cleared Alarms, "Held" Alarm Notifications, "Alarm Disposition Unknown" Messages, Follow-Up Manager Inquiries, Configuration Updates, Log Updates, and Event Profile Updates (parameterized as described below).
Control: Disposition rules and Suspend/Resume.
Parameterization: Event Profile Updates (enable and disable commands) are parameterized by the selection of the **Enable/disable Event Profile Action** optional operational feature.

A235 Identify Alarm Destinations

Description: The activity determines destinations to which **Reported Alarms**, **Cleared Alarms**, and **"Alarm Disposition Unknown" Messages** should be sent. The outputs are sent to the activity **Process Outgoing Messages.**

Input: Reported Alarms, Cleared Alarms, and "Alarm Disposition Unknown" Messages.
Output: The same as the inputs with intended destinations in the communications network.
Control: "Alarm to Destination" Mappings are provided to associate particular inputs with destinations.
Parameterization: None

5.2.5 Fourth-Level Decompositions

This section describes selected fourth-level decompositions for the activities described in section 5.2.4. These include decompositions for Activity A231 **Analyze Poll Responses** and Activity A233 **Correlate Events.** Third-level decompositions of other second-level activities was not deemed necessary.

5.2.5.1 Decomposition of Analyze Poll Responses

This decomposition describes the breakdown of Analyze Poll Responses activity shown as activity A231 in figure 5.6. Three more specific activities are described:

- o A2311 Compare Responses
- o A2312 Apply Polling Analysis Rules
- o A2313 Accumulate Poll Response Statistics

Activity A2313 is parameterized by selection of optional feature **Automatic Control of Polling Time Interval.** This activity is also specialized to activity A2313a or A2313b by the selection of **Consolidated** or **Partitioned** alternative operational features. The decomposition is shown in figure 5.7a. Specialization of activities is shown in figure 5.7b.

A2311 Compare Responses

This activity compares **poll responses** to a **Network Resource Identification Data List** to identify what network resources are not responding to polls.

Description: The activity accumulates **match results** showing responses and non-responses for a set of network devices that have been polled over a specified polling time interval or intervals. Responses consist of **PING-type poll responses, GET-type poll responses,** and **Polled alarm notifications** (responses that provide detailed descriptions of faults). At predetermined time intervals (based on the **polling time interval),** match results are forwarded to (1) Activity A2312 to for application of polling analysis rules and (2) Activity A2313 to compile **Poll Response Statistics** (if optional features are selected that parameterize this activity). **Suspend/Resume** controls if the activity is off and on.

Input: PING-type poll responses, GET-type poll responses, Polled Alarm Notifications, and Network Resource Identification Data Lists.
Output: Match Results
Control: Polling Time Interval and Suspend/Resume.
Parameterization: None

A2312 Apply Polling Analysis Rules

This activity applies polling analysis rules to incoming **match results** to identify alarm conditions and issue **alarm notifications.**

Description: Polling Analysis Rules can be used specify the conditions under which a lack of response to polls (or a **Polled Alarm Notification)** requires the issuance of an **Alarm Notification.** These rules are applied to **Match Results** produced by activity A2311. The output is an **Alarm Notification. Suspend/Resume** is a control that turns the activity off and on.

Input: Match Results
Output: Alarm Notifications
Control: Polling Analysis rules and Suspend/Resume.
Parameterization: None

Figure 5.7a: Decomposition of Analyze Poll Responses

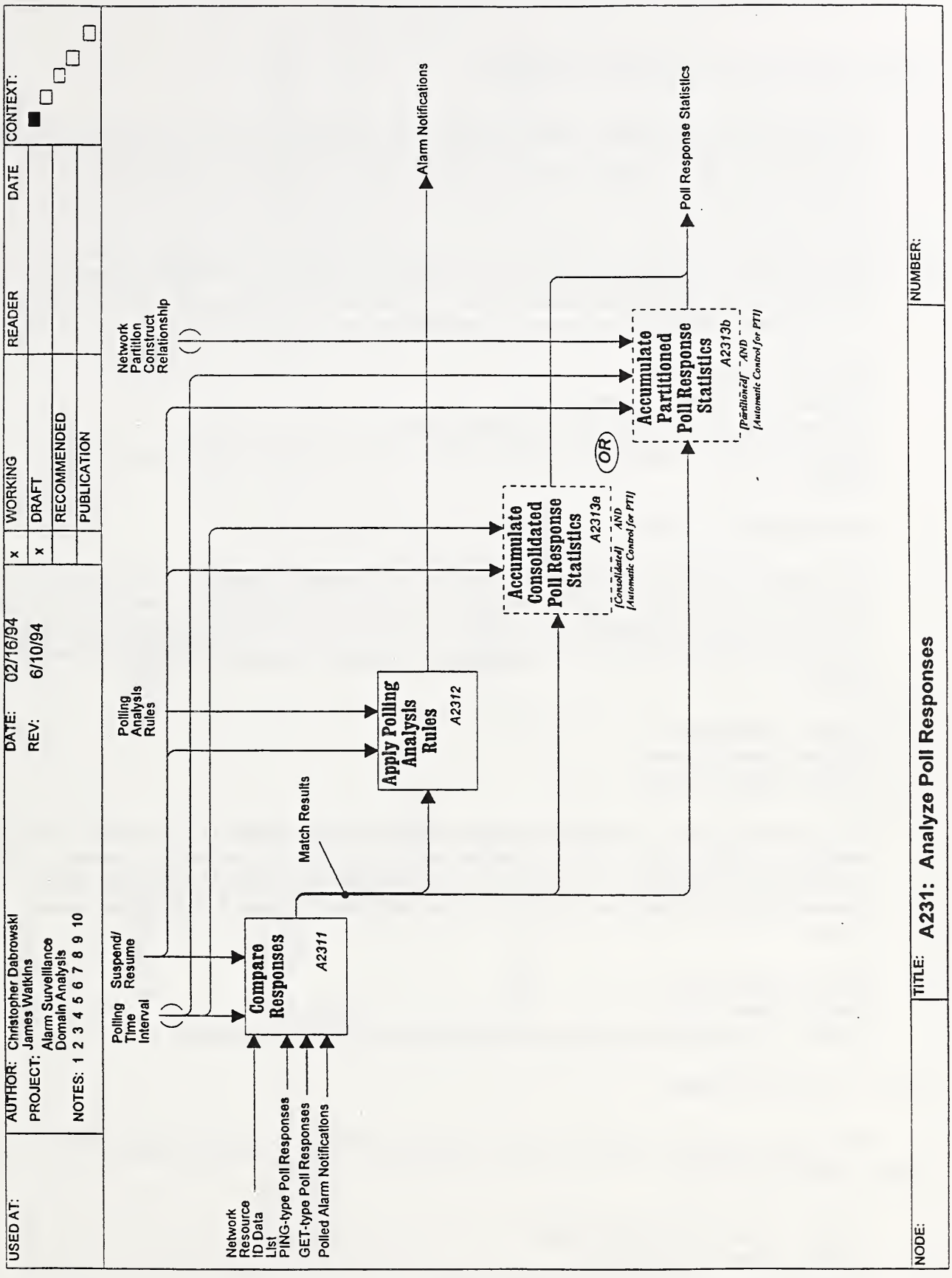


Figure 5.7b: Decomposition of Analyze Poll Responses (specialized)

A2313 Accumulate Poll Response Statistics

This activity accumulates **Match Results** for poll responses over a specified period of time and forwards these accumulated responses for automatic computation of the polling time interval (PTI). The activity is parameterized as described below.

Description: The activity accumulates statistics on **Match Results** for a set of network devices that have been polled over a specified polling time interval or intervals. Accumulated responses are forwarded to activity A3--**Poll Agents**--to allow calculation of the polling time interval (PTI) by activity A31, **Determine Polling Time Interval**. **Suspend/Resume** controls if the activity is on or off.

Input: Match Results
Output: Poll Response Statistics
Control: Polling Time Interval and Suspend/Resume.
Parameterization: Selection of **Automatic Polling Time Interval Control** optional operational feature.

Specialization: The activity may specialized in two ways:

(1) as activity A2313a, **Accumulate Consolidated Poll Response Statistics**. This activity accumulates statistics for a set of devices that are organized according to the consolidated monitoring organization. This specialization is determined by selection of the **Consolidated Monitoring Organization** optional operational feature (in addition to selection of the **Automatic Control of Polling Time Interval** feature).

Input: Same as above.
Output: Same as above.
Control: Same as above.

(2) as activity A2313b, **Accumulate Partitioned Poll Response Statistics**. This activity accumulates statistics for multiple sets of devices organized using the partitioned monitoring organization. This specialization is determined by selection of the **Partitioned Monitoring Organization** optional operational feature (in addition to selection of the **Automatic Control of Polling Time Interval** feature).

Input: Same as above.
Output: Same as above.
Control: Polling Time Interval and Network Partition Construct Relationship.

5.2.5.2 Correlate Events

This decomposition of activity A233 **Correlate Events**, shown in figure 5.6, consists of three specific activities:

- A2331 Apply Correlation Rules
- A2332 Form Log Inquiry
- A2333 Maintain Active Correlation Data

These activities are not parameterized. The decomposition is shown in figure 5.8.

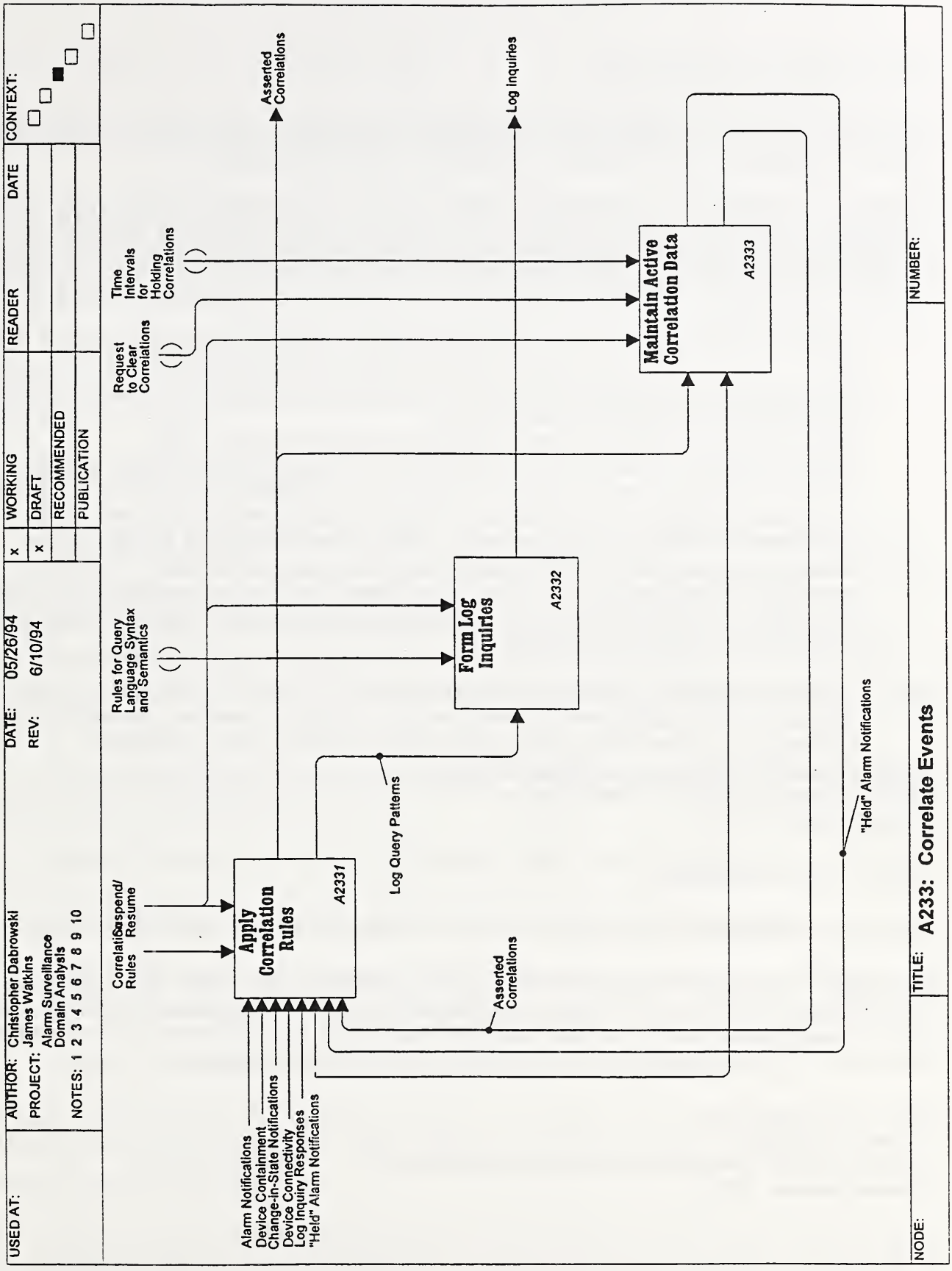


Figure 5.8: Decomposition of Correlate Events

A2331 **Apply Correlation Rules**

The activity applies correlation rules to incoming Event Notifications to assert correlations. Asserted correlations are forwarded to **Determine Alarm Disposition.**

Description: The activity applies **Correlation Rules** to incoming **Event Notifications**--both **Alarm Notifications** and **Change-in-State Notifications**--to correlate them with previous Event Notifications and previously asserted correlations. Correlations are asserted for Event Notifications occurring on the same or related set of resources over a specified time interval. This includes the following types of correlations:

- o Multiple occurrences of same alarm notification, including a specified number of alarms of a particular type.
- o Multiple occurrences of different alarm notifications that either (1) belong to a common supertype (generalization) or (2) satisfy a boolean pattern.
- o Multiple occurrences of change-in-state notifications and other non-alarm events.
- o Multiple occurrences of change-in-state notifications and alarm notifications. Where necessary, information about the network configuration is used in the correlations. This includes configuration information describing **Network Resources, Connectivity Relationships** among resources, and **Containment Relationships** among resources. **"Held" Alarm Notifications** are also correlated. When necessary, rules may also initiate **Log Inquiries** to retrieve historical information needed for correlations. This is done by issuing a **Log Query Pattern** that specifies the criteria for the query. The pattern is provided to activity A2332 in order to formulate the query. **Suspend/Resume** is a control that turns the activity off and on.

Input: (1) Alarm Notifications, (2) Change-in-State Notifications, (3) Device Connectivity and Device Containment Relationships between network resources involved in correlation operations, (4) Results of Log Inquiries, (5) "Held" Alarm Notifications, and (6) previously asserted correlations.
Output: Asserted Correlations and Log Query Patterns.
Control: Correlation Rules and Suspend/Resume.
Parameterization: None

A2332 **Form Log Inquiry**

The activity formulates a log inquiry to retrieve needed information from an event log.

Description: The activity receives from A2331 a **Log Query Pattern** that will match data needed for a correlation activity and forms a log inquiry. A **Log Inquiry** is formed according to the syntactic and semantic rules of a query language used by the target event log. The log inquiry is then forwarded to an agent system responsible for a log. **Suspend/Resume** is a control that turns the activity off and on.

Input: Log Query Pattern
Output: Log Inquiry
Control: Rules for query language syntax and Suspend/Resume.
Parameterization: None

A2333 **Maintain Active Correlation Data**

The activity maintains "held" alarm notifications, results from previous correlations, and other pertinent information to be reused in subsequent correlations.

Description: The activity accepts **"Held" Alarm Notifications** and **Asserted Correlation** and maintains them to reuse as input to subsequent correlation actions of Activity A2331. This data is provided on request to Activity A2331. "Held" alarms and correlations are discarded after specified time interval is exceeded or in response to external request to clear correlation data and Suspend/Resume. Such requests may be associated with mode change commands.

Input: Asserted Correlations and "Held" Alarm Notifications.
Output: Previously asserted correlations and "Held" Alarm Notifications.
Control: Request to Clear Correlations, time intervals for holding correlations, and Suspend/Resume.
Parameterization: None

5.3 State Transition Diagrams

This section provides state transition diagrams for selected IDEF0 activities in the decomposition. That is, for particular IDEF0 activities, this section specifies the individual states that the activity may enter into and transitions that occur between states. This information describes how a particular activity performs its function. As such the state transitions diagrams for a particular activity are internal to that activity and as such are transparent to other activities. Interactions between activities are limited to data flows and control flows.

The state transition diagramming technique is based on a simple finite state machine (FSM) model. This model consists of:

- States in which the activity is performing a specific task or is idle.
- State Transitions in which the activity ends one state and begins another.
- Events that trigger state transitions: either the arrival of data needed to perform the activity, the elapse of a time interval, completion of a task, or other occurrence.
- Outputs that are emitted by the activity as a result of a state transition.

The next step in detailing the activities would be to describe procedures for the tasks performed within individual states. This is beyond the current funding resources of the Domain Analysis Case Study.

Each activity for which state transitions are provided is a "leaf node" activity that is not decomposed further. Due to limitations in funding and time constraints, the selected activities were limited to those that apply event profiles and analysis rules. These include:

- o A231 Filter Events
- o A2322 Apply Polling Analysis Rules
- o A2331 Apply Correlation Rules
- o A234 Determine Alarm Disposition

5.3.1 States for Filter Events

This section describes the states associated with Activity A231, **Filter Events.** The state transition diagram for this activity is shown in figure 5.9. States and state transitions in this diagram are described below.

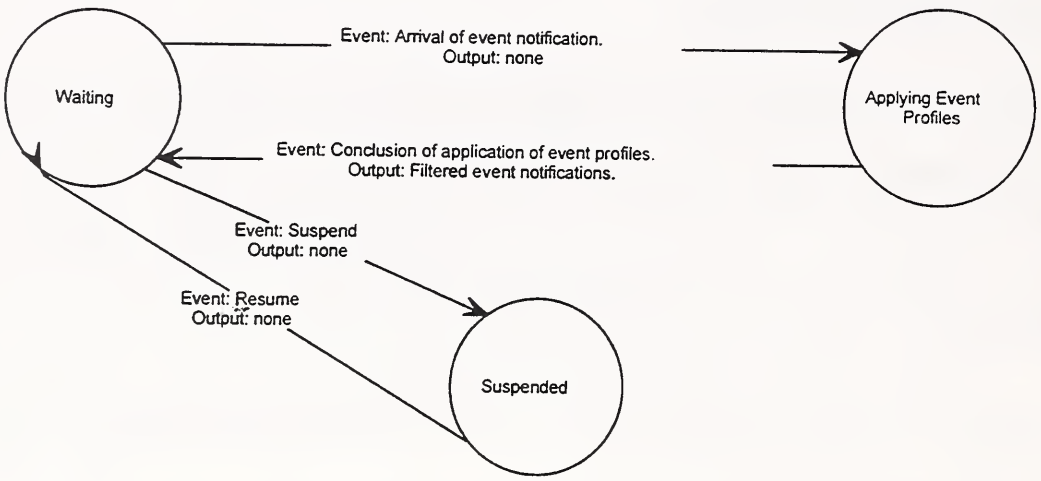


Figure 5.9: State transitions for Filter Events

STATES:

1. **Waiting**

   Description: The activity waits for an Event Notification to which event profiles can be applied.

2. **Applying Event Profiles**

   Description: The activity applies Event Profiles to filter Event Notifications.

3. **Suspended**

   Description: The activity is suspended by an externally issued command.

STATE TRANSITIONS:

Transition 1: Waiting to Applying Event Profiles

Event: Arrival of Event Notification.
Output: None

Transition 2: Applying Event Profiles to Waiting

Event: Conclusion of application of event profiles.
Output: Filtered Event Notifications, if Event Notification is successfully filtered. These are forwarded to either activity A233 **Correlate Events** (for Event Notifications that must be analyzed further) or to A24 **Identify Alarm Destinations** (for Reported Alarms or Cleared Alarms).

Transition 3: Waiting to Suspended

Event: Arrival of a **suspend** command from either the network administrator or Activity A211 **Coordinate Construct Control Commands.**
Output: None

Transition 4: Suspended to Waiting

Event: Arrival of a **resume** command from either the network administrator or Activity A211 **Coordinate Construct Control Commands.**
Output: None

Transitions from the **Applying Event Profiles State** to **Suspended** or assumed not to occur in this model, but could be added if necessary.

5.3.2 States for Apply Polling Analysis Rules

This section describes the state transition diagram for Activity A2312, **Apply Polling Analysis Rules**. This diagram appears in figure 5.10. States and state transitions are described below.

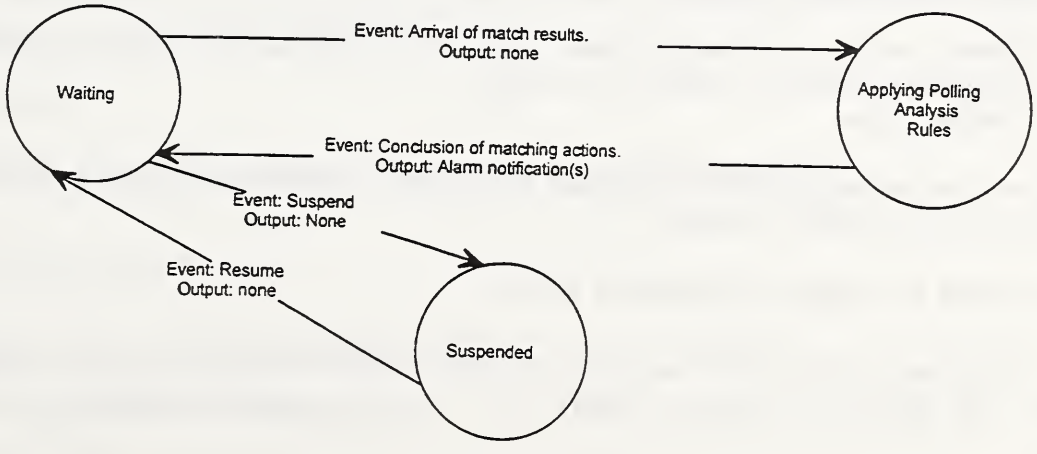


Figure 5.10: State transitions for Apply Polling Analysis Rules

STATES:

1. **Waiting**

   Description: The activity waits for an arrival of **Match Results** of a set of polling responses.

2. **Applying Polling analysis Rules**

   Description: The activity applies polling analysis rules to the match results to determine if an alarm notification should be issued.

3. **Suspended**

   Description: The activity is suspended by an externally issued command.

STATE TRANSITIONS:

Transition 1: Waiting to Applying Polling analysis Rules

Event: Arrival of match results.
Output: None

Transition 2: Applying Polling Analysis Rules to Waiting

Event: Conclusion of matching actions.
Output: Alarm notification(s), if successful match occurs.

Transition 3: Waiting to Suspended

Event: Arrival of a **suspend** command from either the network administrator or Activity A211 **Coordinate Construct Control Commands.**
Output: None

Transition 4: Suspended to Waiting

Event: Arrival of a **resume** command from either the network administrator or Activity A211 **Coordinate Construct Control Commands.**
Output: None

Transitions from the **Applying Polling Analysis Rules State** to **Suspended** or assumed not to occur in this model, but could be added if necessary.

5.3.3 States for Apply Correlation Rules

This section describes the state transition diagram Activity A2331, **Apply Correlation Rules**. The diagram is shown in figure 5.11. States and state transitions are described below.

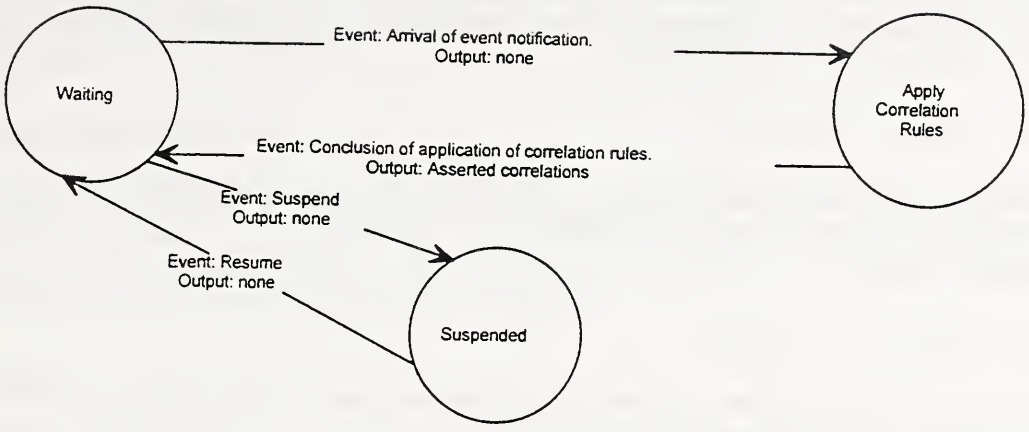


Figure 5.11: State transitions for Apply Correlation Rules

STATES:

1. **Waiting**

   Description: The activity waits for an Event Notification to be correlated.

2. **Applying Correlation Rules**

   Description: The activity applies correlation rules to an Event Notification. In this state, the activity determines whether the Event Notification (either an Alarm Notification or Change-in-State Notification) can be correlated to previous alarm notifications, Change-in-State Notifications, Asserted Correlations, or "Held" Alarm Notifications.

3. **Suspended**

   Description: The activity is suspended by an externally issued command.

STATE TRANSITIONS:

Transition 1: Waiting to Applying Correlation Rules

Event: Arrival of Event Notification.
Output: None

Transition 2: **Applying Correlation Rules** to **Waiting**

Event: Conclusion of application of correlation rules.
Output: (1) Asserted Correlations, if successful match occurs. These are forwarded to **Determine Alarm Disposition** and to **Maintain Active Correlations**. (2) Log Query Patterns (forwarded to activity A2332 **Form Log Inquiries**.

Transition 3: **Waiting** to **Suspended**

Event: Arrival of a **suspend** command from either the network administrator or Activity A211 **Coordinate Construct Control Commands.**
Output: None

Transition 4: **Suspended** to **Waiting**

Event: Arrival of a **resume** command from either the network administrator or Activity A211 **Coordinate Construct Control Commands.**
Output: None

Transitions from the **Applying Correlation Rules State** to **Suspended** or assumed not to occur in this model, but could be added if necessary.

5.3.4 State Transitions for Determine Alarm Disposition

This section describes the state transition diagram for Activity A234, **Determine Alarm Disposition.** This activity is shown in figure 5.12. States and state transitions are described below.

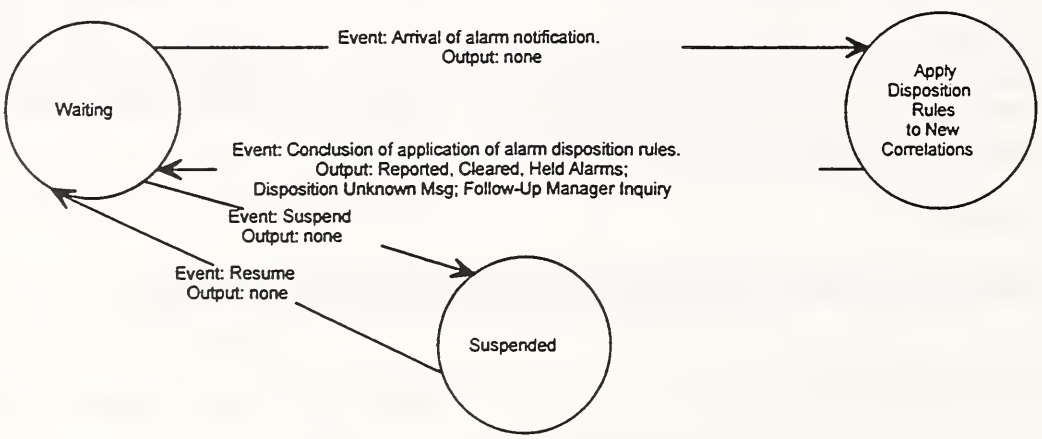


Figure 5.12: State transitions for Determine Alarm Disposition

STATES:

1. **Waiting**

   Description: The activity waits for the arrival of an alarm notification whose disposition must be determined.

2. **Applying Disposition Rules**

   Description: The activity applies disposition rules to the alarm notification. The application of alarm disposition rules determines whether the alarm notification should be reported, cleared, "held" for subsequent correlation, or whether a Follow-Up Manager Inquiry should be issued. If no disposition can be determined, this in itself becomes the determination.

3. **Suspended**

   Description: The activity is suspended by an externally issued command.

STATE TRANSITIONS:

Transition 1: Waiting to Applying Disposition Rules

Event: Arrival of alarm notification.
Output: None

Transition 2: Applying Disposition Rules to Waiting

Event: Conclusion of application of alarm disposition rules.
Output: (1) Reported Alarm, Cleared Alarm, "Held" Alarm Notification, or "Alarm Disposition Unknown" Message, if successful match occurs. (2) Data for Follow-Up Manager Inquiry, if successful match occurs. This is forwarded to activity A4 **Process Outgoing Messages.**

Transition 3: Waiting to Suspended

Event: Arrival of a **suspend** command from either the network administrator or Activity A211 **Coordinate Construct Control Commands.**
Output: None

Transition 4: Suspended to Waiting

Event: Arrival of a **resume** command from either the network administrator or Activity A211 **Coordinate Construct Control Commands.**
Output: None

Transitions from the **Applying Disposition Rules State** to **Suspended** or assumed not to occur in this model but could be added if necessary.

6. THE INFORMATION MODEL

This section presents the Information Model for Alarm Surveillance. The Information Model describes the major data structures--both entities and relationships--that will be needed to perform the alarm surveillance system function. This Model contains common structures--those needed by all systems within the alarm surveillance domain--as well as structures that will be needed to support functions specific to subsets of systems in the domain. The parameterization of specialized structures is indicated in the descriptions.

The Information Model was developed using the Culture semantic modeling language. This language and other notational conventions are described in the first subsection. This is followed by an overview of the Information Model, provided in section 6.2. The last three subsections provide more detailed descriptions of the major subcomponents of the Information Model: network management communications support structures in section 6.3; alarm surveillance control structures in section 6.4; and managed resource and network configuration support structures in section 6.5.

6.1 The Modeling Representation

The modeling representation chosen is based on the Culture modeling method, developed by ASTEC in Crofton, Maryland [ASTEC90]. Culture is a semantic modeling approach that combines concepts derived from linguistics with the extended entity-relationship diagramming technique. The entity-relationship models presented below incorporate a number of Culture features.

- Type hierarchies of entity and relationship types are used. Within the hierarchy, more general types are used to define more specific types. More specific subtypes inherit characteristics of more general supertypes. This feature is consistent with the FODA approach as described in [KANG90].

- The binary relationship model is extended to allow definition of "n-ary" relationships. Relationship roles define each of the "n" components of an "n-ary" relationship. The types of objects that can be allowed in each role, called role players, are specified together with minimum and maximum number of objects. Individual roles can be optional or mandatory. Relationship cardinality is described using the notations (1) for one, (M) for many, and (1-M) for one-to-many.

- It is also possible to assign combinations of objects to play roles in a relationship. The "participation set" construct is used to group role players into mutually exclusive sets. In this document "participation sets" are sometimes simply referred to as "sets."

- In addition to having relationships between entities, it is possible to have direct relationships between relationships types. That is, relationship roles can be played by either relationships or entities.

- In Culture, both entities and relationships may have properties, or attributes. In addition, when objects are role players for particular roles, they may have additional properties assigned to them.

Culture largely fulfills the requirements of FODA for representing the Information Model as described in [KANG90]. Readers interested in a more complete description of Culture should refer to [ASTEC90]. In the Culture diagrams in this document, entities are represented by rectangles, relationships are represented by diamond shapes, and roles are noted next to the arcs. Parameterized variable entities and relationships are indicated by an asterisk "*".

6.2 Information Model Overview

A diagram shown in figure 6.1 provides an overview of the structure of information needed to support the alarm surveillance activity as performed by managers. The structural information provided in this diagram and the more detailed diagrams found later in this section support the data flows shown in the IDEF0 diagrams in section 5. The information in figure 6.1 shows the essential relationships involved in the transmission of manager inquiries from managers to agents who are responsible for resources within a communications network. The figure also shows the relationships associated with transmission of event notifications by agents describing the status of resources and information about faults (which may or may not occur as a result of manager inquiries). Also shown are relationships between managers, event profiles, and patterns. Event profiles consist of patterns against which incoming event notifications are matched and filtered to eliminate irrelevant messages and identify genuine alarms that affect the status of network resources. Similarly, correlation of event notifications and determining the disposition of alarm notifications is also accomplished by matching against patterns. Finally, entities and relationships are shown that depict the structure of information for reporting alarms to managers and agents who require this information. Specializations of the entities and relationships in this diagram are described in later subsections.

Information Structures That Support Network Management Communications

The heart of this diagram shows the information structures for the communications between agents and manager systems. Agent systems are responsible for handling agent/manager communications on behalf of individual network resources being monitored. This is described by the **agent responsibility** relationship (or using the verb form, the "agent responsible for" relationship). The relationship has two roles: the *agent for* role is played by the **agent** entity; the *managed resource of* role is played by the **network resource** entity. In the diagram, communications between managers and agents are represented using three specializations of the generalized **transmission** (or using the verb form, the "transmits")

relationship: **manager inquiry transmission**, **agent transmission**, and **alarm disposition report transmission**.

The **manager inquiry transmission** relationship describes a message sent by a manager to one or more agents requesting information on the status of resources agents may be responsible for. In this relationship, the *sender* role is played by the **manager** entity. The *receiver* role is played by the agent entity. The *message* role is played by the **manager inquiry** entity, which is the information request. Both the entities and relationships associated with agent/manager communications are specified in greater detail in section 6.3. In response to manager inquiry transmissions, an agent system may send an event notification to one or more managers describing detected alarms and changes in the status of the resources they are managing. This is described by the **agent transmission** relationship. In this relationship, the *sender* role is played by the **agent**, the *receiver* role by the **manager** entity, and the *message* role by the **event notification** entity. Event notifications may be sent by agents on their own initiative as well as in response to manager inquiries. (Cause and effect is shown in the state-transition diagrams.)

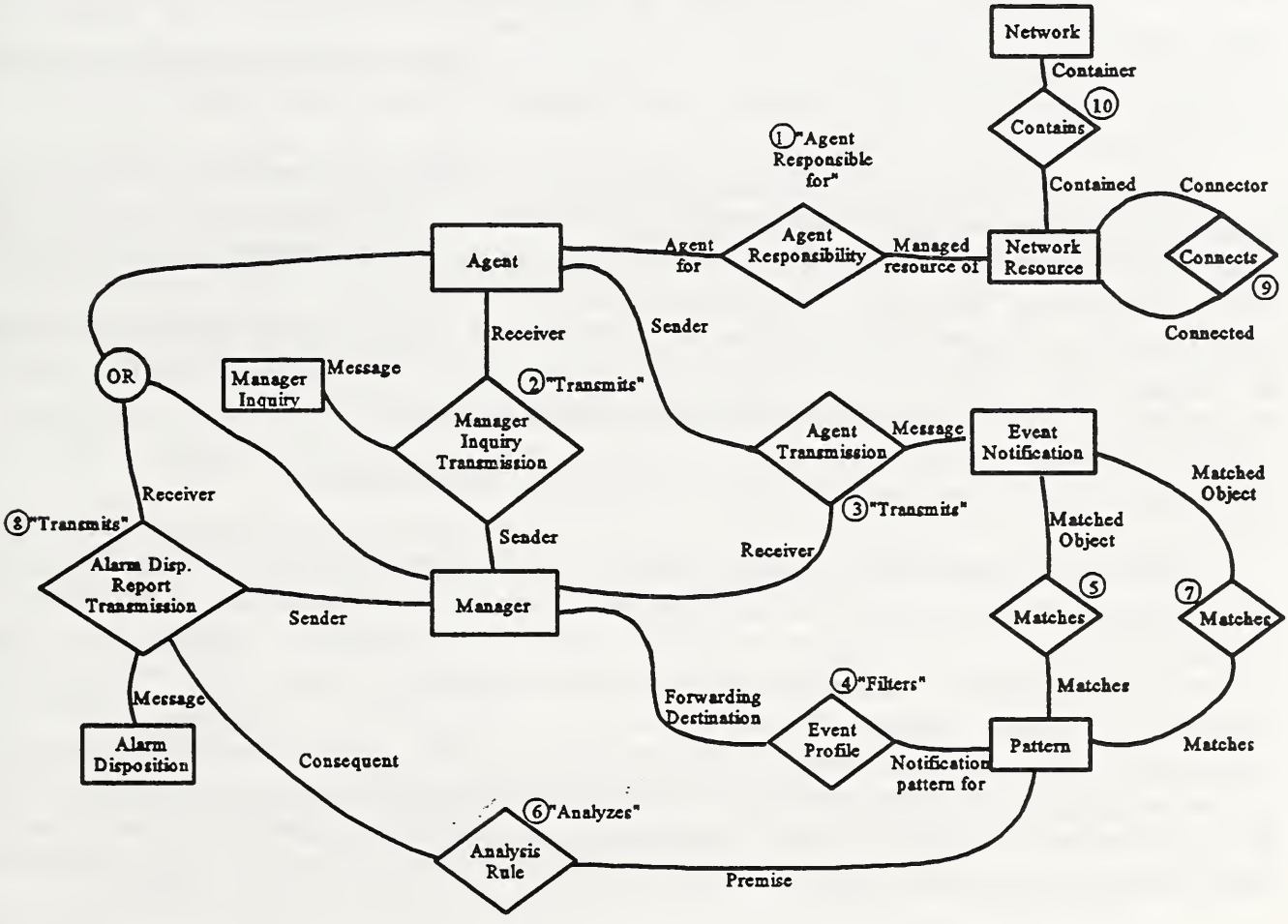


Figure 6.1: Information Model Overview

Information Structures For Analysis and Intelligent Surveillance

Once event reports are received by the manager, they are filtered and analyzed to identify alarms representing problems that need to be reported to network administrators. Filtering is accomplished by using patterns to match event notifications sent by agents. This is depicted in the **event profile** relationship which describes the filtering structure and **matches** relationship which represents the filtering action itself. In the **event profile** (or "filters") relationship, the *notification pattern for* role is played by a **pattern construct** entity; the *forwarding destination* role is played by the **manager** entity. In the **matches** relationship, the roles specify a **pattern** entity that has matched an **event notification** entity. Analysis consists of correlating filtered event notifications and determining what action to take on correlated notifications. The information constructs necessary to support the analysis activity are generalized into the **analysis rule** (or "analyzes") relationship. In this relationship, the *premise* role denotes **pattern construct** entities that match filtered event notifications. The *consequent* role is played by an instance of **alarm disposition report transmission** relationship--indicating that this transmission is the result of the analysis performed. The specialization of **analysis rule** is described in section 6.4. Information structures needed by some application systems to organize event profiles and analysis rules are also described in this section. Section 6.4 also defines the **network partition** relationship (not shown in figure 6.1), which is used to organize **network resources** into sets to be treated separately for monitoring, filtering, and analysis purposes.

The reporting of event notifications that have been filtered and analyzed is represented by the **alarm disposition report transmission** relationship. In this relationship, the *sender* role is played by the **manager** entity; the *receiver* role may be played by **manager** entity as well (a different instance of the entity)--representing a network administrator. The *receiver* role may also be played by an **agent** entity--representing other persons and systems that must be informed; the *message* role is played by the **alarm disposition** entity. The **alarm disposition report transmission** relationship is described in greater detail in section 6.3.

Information Structures That Represent the Network Configuration

To perform the analysis activity properly requires knowledge of the relationships that exist between network resources in the managed network. The **connection** and **containment** relationships shown in the diagram provide a basis for describing the configuration of the communications network that is managed by an alarm surveillance system. The roles for these relationships denote **network resources** that are connected or contained, respectively. Connection refers to physical links existing between resources. Containment relationships are at a more logical level, such as between a group of resources that belong to a network. Both the specializations of network resource types and the specialization **connection** and **containment** relationships are described in greater detail in section 6.5 **network configuration structures**.

Within sections 6.3, 6.4, and 6.5, the specializations of the major entity and relationship types are provided. Each entry for an individual entity or relationship type includes a description of the entity or relationship, an identification of its most important attributes, the

source of information about the entity, and further specializations that can occur if any. (Due to budgetary limitations, a detailed description of all entity attributes was felt to be beyond the scope of this study.) For relationship types, a concise summary of the information needed for its Culture representation is provided. For parameterized information structures, the optional or alternative feature whose selection parameterizes the structure is indicated.

6.3 Communications Support Structures

Communications support structures include entities that describe managers, agents, and the types of messages they exchange. Culture n-ary relationships are used to capture the notion of the transmission of a specific type of message from a particular source to a particular destination. This includes manager inquiries to obtain information about the status of devices (including polls); Event notifications issued by agents (including responses to manager inquiries, alarm notifications, and change-in-state notifications); and manager reports that forward selected information about alarms to destinations in the network. The entities and relationships described in this section are summarized graphically in the figures below.

6.3.1 Description of Entity Types

There are three entity types: (1) Communicating entities are managers and agents (as described above), (2) Manager inquiries are sent by managers to request information from an agent, and (3) Event notifications are sent by agents to report the state of a device. Manager inquiries and event notifications correspond to particular data flows in the Functional Model.

6.3.1.1 Communicating Entities

Description: Communicating entities use the communications services provided by the network to transmit messages, including manager inquiries and event notifications, described below.

Attributes: **Network address** contains the address (logical or physical to which messages may be sent). **Active** is a boolean attribute that describes whether or not the entity is operating.

Source: [GTE93b]

a) Manager

Description: This entity represents a manager system that runs on a network device.

b) Agent

Description: This entity represents an agent system that runs on a network device.

6.3.1.2 Message Entities

Description: This entity describes the contents of messages that are sent between managers and agents. The entity is specialized extensively, as described below.

Attributes: The attribute **time** contains the time at which the inquiry was sent.

a) Manager Inquiry

Description: A manager inquiry is sent by a manager to an agent to obtain information about the network device that the agent is responsible for.

Source: [GTE93b]

a.1) PING-type Poll*

Description: PING-type polls are short messages intended to determine if a particular agent system is up or down.

Parameterization: Selection of **PING-type** Poll Message Optional Operational Feature.

a.2) GET-type Manager Inquiry

Description: The entity represents information about requests for values of one or more specific variables that describe the status of network devices. The entity may describe the variable values requested in a **GET-type poll** message. The entity may also represent device variables and values requested in a **Follow-Up Manager Inquiry**. In the SNMP or CMIP management protocols, the GET-Type Manager Inquiry is a GET operation that retrieves internal device variables.

Additional Specialization: This entity can have many different specializations. In alarm surveillance applications, the content of an individual Follow-Up Manager Inquiries varies greatly depending on the needs of specific applications.

b) Event Notification

Description: This entity describes the structure of information in messages transmitted by agents, describing the status of the devices they are responsible for. Event notifications are sent by agents to managers.

Source: [GTE93b], [ISO/IEC 10165-2], [ROSE90a], [ROSE90b], and [ROSE91]

b.1) Solicited Event Notifications

Description: A response by an agent to a manager inquiry (either a **PING-type poll** or **GET-type manager inquiry**).

b.1.1) PING-type Poll Response

Description: This entity represents a response to a **poll** sent by an agent. This would be a PING-type poll indicating the device the agent is responsible for is currently operational. (In Internet suite of protocols, such a message would be sent using an ICMP packet.) This entity corresponds to the data flow **PING-type Poll Response**.

b.1.2) Manager Inquiry Response

Description: This entity contains a sequence of device status variables and their values. For networks that are compliant with either the SNMP or CMIP/CMISE management protocols, these are Management Information Base (MIB) variables. A manager inquiry response entity may contain information that represents **Responses to Follow-Up Manager Inquiries** or **GET-Type Poll Responses**.

Additional Specialization: This entity can be greatly specialized. In alarm surveillance applications, the content of **Responses to Follow-Up Manager Inquiries** and **GET-Type Poll Responses** vary greatly depending on the needs of specific applications.

b.2) Unsolicited Event Notifications

Description: An event notification issued by an agent system that contains information describing its status. Event notifications may describe alarm situations existing on devices or may describe changes in status.

b.2.1) Change-in-State Notification Entity

Description: An unsolicited event notification that reports a change in the value of one or more internal variables that describe the state of a network device. A change-in-state notification entity may not necessarily convey information that is related to a recognized fault.

Attributes: The **cause** attribute indicates why the notification was issued. The notification may have been issued by the agent system for the device, due to manual intervention or for unknown reasons.

b.2.1.1) Change-in-Operability State Entity

Description: The entity describes a report of an action relating to physical installation and working condition of a network resource. It may be used to change the operation of any surveillance construct.

Attributes: **Event** indicates whether the resource is being (or is to be) enabled or disabled.

b.2.1.2) Change-in-Usage State Entity

Description: The entity describes a report of whether a network resource is in use and possibly whether it has any spare capacity.

Attributes: **Event** is an attribute that indicates whether a new user commences use of a network resource, a user terminates usage of the resource, if there is an increase in maximum capacity of resource, or if there is a decrease in maximum capacity of resource.

b.2.1.3) Change-in-Attribute Value Entity

Description: The entity describes a report of a change in value of an attribute for a particular network resource.

Attributes: **Attribute name** contains the name of the attribute to be modified. **Old value** and **new value** contain the old values and new values respectively.

b.2.2) Alarm Notification Entity

Description: An alarm notification entity conveys information about a possible detected fault. Alarm notifications represent input to the alarm surveillance system coming from the communications network context. An alarm notification entity may include information about the type of fault that has been detected, information about the circumstances surrounding the fault, and an estimate of the severity of the fault. A list of the types of faults that may be sent is currently found in the Feature Model--in section 4.2, Context Features.

Attributes: The attributes are derived from the ISO/IEC Alarm Reporting Function Standards Profile (ISO\IEC 10164-4, sec. 8.1.2). **Event type** describes the type of fault that has been detected. Possible fault types are environmental, equipment, communications, processing, performance (quality of service). **Probable cause** provides a more detailed description of the fault. **Perceived severity** describes how severe the fault is. Levels of severity include: "indeterminate," "critical," "major," "minor," "warning," and "cleared."

Source: [ISO\IEC 10164-4]

Additional Specialization: The alarm notification entity may be specialized to reflect the type of information that may be provided by agent systems in specific communications network contexts. The specializations may include attributes derived from [ISO\IEC 10164-4], four of which are described below. Attributes needed to describe threshold information include **threshold level**, the level at which a threshold is triggered; **observed value**, the recorded value; and **arm time**, the clock time at which the threshold level was reset. **Additional text** is a text field with additional descriptive information.

6.3.2 Description of Relationship Types

There is one general class of relationships for the entities defined in the preceding section: Transmissions. This class of relationships defines messages that are exchanged between managers and agents and between managers and other managers. There are three roles: **sender**, **receiver**, and **message**. This general class may be defined as the relationship **Transmission**:

Description: The **sender** and **receiver** roles are constrained to **communicating entities**. The **message** role is played by any **message** entity described in section 6.3.1.2.

3-ary Transmission	
Sender:	(1-M) Communicating Entity
Message:	(1) Message
Receiver:	(1-M) Communicating Entity

More specific relationship subtypes described below constrain these messages to particular types of objects. Transmission relationships are shown in both figure 6.2.

Source: [GTE93a] and [GTE93b]

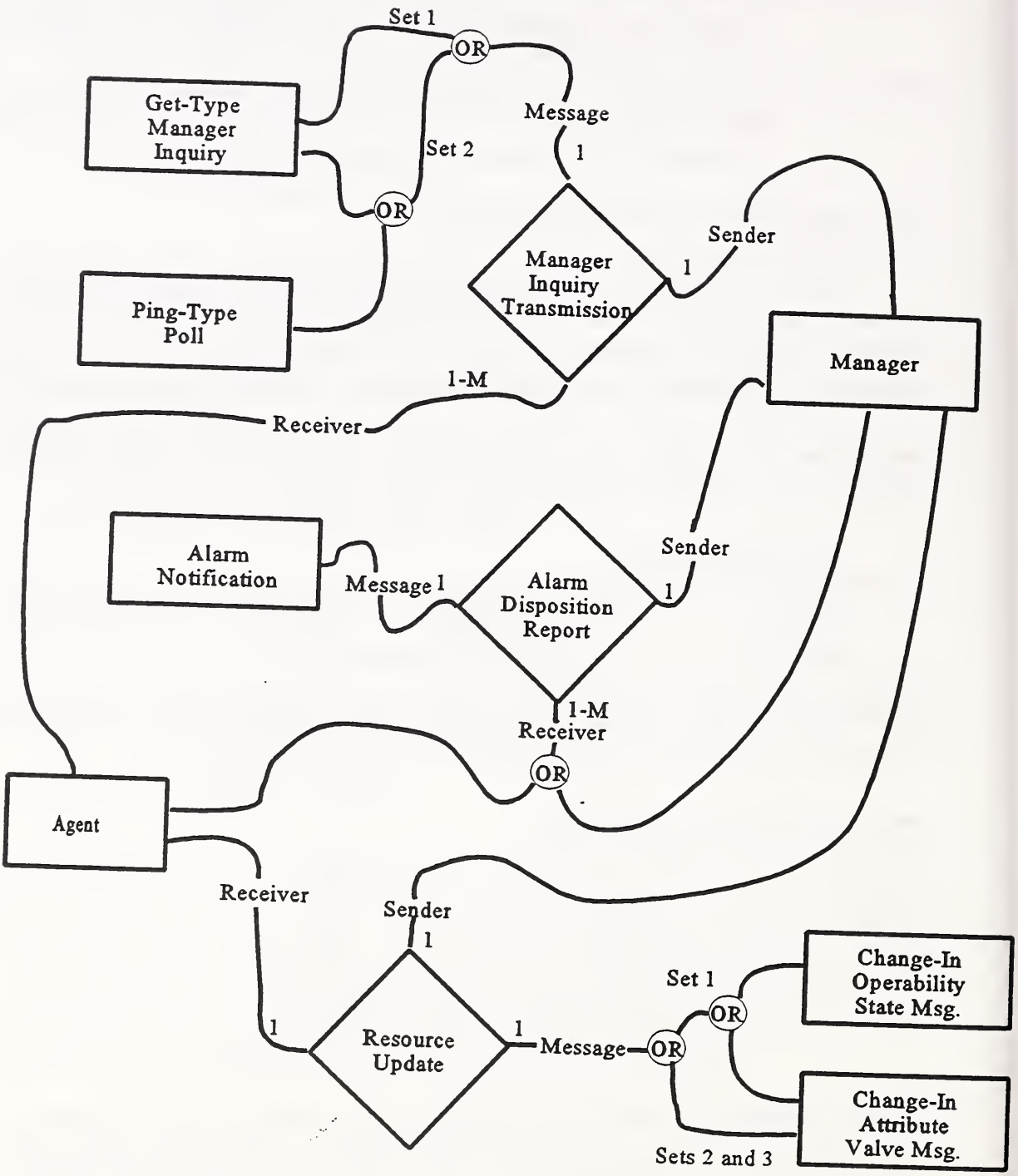


Figure 6.2: Specializations of the Manager Transmission

6.3.2.1 Agent Transmission

Description: This is a relationship that describes the transmission of an event notification from an agent to a manager. The **sender** role is constrained to an **agent** entity. The **message** role denotes the **event notification** that was sent (including any solicited or unsolicited event notification or specialization described in sec. 6.3.1.2 (b)). The **receiver** is constrained to the **managers** to which the message was sent. This relationship appears in figure 6.1

3-ary Agent Transmission

Sender:	(1) Agent
Message:	(1) Event Notification and its specializations
Receiver:	(1-M) Manager(s)

6.3.2.2 Manager Transmission

Description: This relationship defines messages that a manager may send to agents, network administrators, other managers, end users, and other destinations on the network. **Sender** is constrained to the manager system sending the message. **Receiver** roles are played by both managers and agents as described below in the specializations of this relationship. The **message** role is described separately for each specialization, and is shown in figure 6.2.

a) **Manager Inquiry Transmission**

Description: This relationship defines inquiries into the state of a network resource that a manager makes to an agent system. **Sender** is constrained to the manager system sending the message. The **message** role is constrained to:

Follow-Up Manager Inquiries. These are requests for additional information made to agent systems.

Polling Messages. These messages consist of polls that can be either PING-type polls or GET-type manager inquiries (used in polling).

Each type of message is associated with a different participation set. The **receiver** role is played by agents that are the target of Follow-Up Manager Inquiries or Polling Messages. This relationship is appears in figure 6.2. The relationship has two Culture participation sets:

Participation Set 1: Follow-up Manager Inquiry.

Sender:	(1) Manager
Message:	(1) GET-type Manager Inquiry
Receiver:	(1-M) Agent

Participation Set 2: Polling Message

Sender:	(1)	Manager
Message:	(1)	PING-type Poll or GET-type Manager Inquiry
Receiver:	(1-M)	Agent

b) **Alarm Disposition Report Transmission**

Description: This transmission relationship describes the report of the disposition taken on an alarm notification by an alarm surveillance system. The report is transmitted to agents, network administrators, other managers, end users, and other destinations on the network. The dispositions taken may be to report the alarm, clear the alarm, "hold" the alarm for further analysis, or indicate that its disposition is unknown. **Sender** is constrained to the manager system sending the message. The **message** role is constrained to **Alarm Notification** entities. **Receiver** role may be played by (1) other managers who may present alarm notifications to network administrators or (2) agents that forward the alarm notifications to trouble tracking systems, system logs, or selected end users. This relationship appears in figure 6.2.

3-ary Alarm Disposition Report Transmission:

Sender:	(1)	Manager
Message:	(1)	Alarm Notification Entity
Receiver:	(1-M)	Manager or Agent

Relationship Attributes: The attribute **action** provides additional information about the manager action. The attribute **action** describes the disposition of the alarm: report, clear, "hold," or disposition unknown.

c) **Resource Update**

Description: This relationship defines updates that a manager may make as a result of analysis activity. **Sender** is constrained to the manager system sending the message. The **message** role is constrained to:

Updates to Network Configuration Database. These messages update the current network configuration to reflect changes in the operating status of network (with change-in-operability state entity) resources and the status of connection and containment relationships (with change-in-attribute-value entity).

SET MIB Variable Commands. This message updates the internal device variable (a Management Information Base variable) in a network resource that specifies where the resource's agent sends event notifications. It corresponds to the SET MIB Variable Command used to control monitoring scope.

Alarm Threshold Update. This message updates a threshold attribute for an alarm notification entity maintained on a network resource.

The **receiver** role is played by (1) other managers or agents who may carry out an construct operation update and (2) agents who may carry out a configuration update. This relationship appears in figure 6.2. There are three Culture participation sets.

Participation Set 1: Updates to Network Configuration Database.

Sender: (1) Manager
Message: (1) Change-in-Operability State Notification Entity or Change-in-Attribute-Value Notification Entity
Receiver: (1-M) Agent

Participation Set 2: SET MIB Variable Commands.

Sender: (1) Manager
Message: (1) Change-in-Attribute-Value Notification Entity
Receiver: (1-M) Agent

Participation Set 3: Alarm Threshold Update.

Sender: (1) Manager
Message: (1) Change-in-Attribute-Value Notification Entity
Receiver: (1-M) Agent

6.4 Surveillance Control Structures

The entities and relationships in this section describe (1) structures for defining event profiles and analysis rules, (2) higher-level structures used to control the operation of event profiles and analysis rules, and (3) structures that support the subdivision of the communications network into partitions that can be monitored separately.

In the alarm surveillance domain, much of the information about filtering and analysis is captured in production rules and implemented as rule-based expert systems. The entities and relationships described in this section are essential structures needed to formulate event profiles and rules. These structures are shown in the figures provided in this section. As this part of the model is specialized, the Knowledge Interchange Format (KIF), [GENES92], will be incorporated into the definitions of the rules.

The organization of event profiles and rules into sets provides the network administrator with the ability to control these structures as a group, activating particular sets in response to changes in operating mode (sec. 4.2.4 of the context features). Network partitions allow

network resources to be placed in separate groups that are monitored differently. Event profile and analysis rule sets together with network partitions support the dynamic surveillance control operational feature (sec. 4.3.4 of the operational features). These structures are shown in the figures below.

6.4.1 Description of Entity Types

6.4.1.1 Construct Pattern

Description: This entity describes patterns used in event profiles and analysis rules. These patterns describe objects to be matched by the event profile or analysis rule. As this part of the model is specialized, the structure of these constructs will conform to expressions defined in the Knowledge Interchange Format (KIF) [GENES92]. (Generally, a KIF expression begins with a word or symbol identifying the type of object in a pattern, followed by a sequence of terms--each of which is either a constant, an individual variable, or a sequence variable.) A pattern is designed to match specific types of data structures for event profiles, network resources, communicating entities, correlation assertions, or other objects. Event profiles and analysis rules may specify one or more pattern entities.

Source: [GENES92], [GOLD93], and [GTE93b]

a) **Event Notification Pattern**

Description: This is a pattern that matches event notifications. Such Event notifications have been translated from binary, parsed, and formatted for analysis.

Additional Specialization: This construct pattern may be further specialized to match the various types of event notifications. See section 6.3.1.2.

b) **Network Resource Pattern**

Description: This is a construct pattern that is intended to match network resources.

Additional Specialization: This construct pattern may be further specialized to match the various types of network resources. See section 6.5.1.2.

c) **Communicating Entity Pattern**

Description: This is a construct pattern that matches communicating entities (managers and agents).

Additional Specialization: This construct pattern may be further specialized to match the various types of communicating entities. See section 6.3.1.1.

d) **Correlation Assertion Pattern**

Description: This is a construct pattern that is used to create asserted correlations. The construct pattern corresponds to the **Correlation Assertion** entity described below (sec. 6.4.1.2). The construct pattern is instantiated by a correlation rule (sec. 6.4.2.3).

Additional Specialization: This construct pattern may be specialized to match the different types of correlation assertions. The specialization is highly dependent upon the context and the application.

e) **Function Pattern**

Description: A construct pattern that begins with a constant that represents the name of a function followed by a sequence of variable terms that represent function arguments. Functional expression patterns are necessary to allow data comparisons in event profiles and analysis rules. The function may be a user-defined function or a standard function (=, /=, >, >=, <, etc.). A argument variable is instantiated from a matching variable in a different pattern.

6.4.1.2 Entities Specific to Analysis Activities

a) **Correlation Assertion**

Description: This entity describes the information contained in a correlation assertion. Correlations may be asserted between unsolicited event notifications (both alarm notifications and change-in-state notifications) that occur on related network resources.

Attributes: The attributes specify information necessary to identify the specific types of event notifications and network resources that are involved in the correlation. Previously asserted correlations may be specified. In some cases, the number of occurrences of a particular type of event notification may be a relevant factor.

Additional Specialization: The expertise of local network administrators and network management experts will be used to define the specific correlations that are relevant to a particular alarm surveillance system.

Source: [GTE93b] and [GOLD93]

b) **Schedule***

Description: This construct is used to specify the times when a filtering or analysis construct is in operation. A scheduling construct may have many variations, one of which is described below.

Attributes: **Operational State** describes whether the schedule is enabled or disabled. The attributes that describe the schedule itself may approximate a two dimensional array where one dimension represents the 365 days of the year; the second dimension represents the 24 hours of the day.

Parameterization: The entity is parameterized by the selection of the optional operational feature, **Scheduling**.

Source: [GTE93b]

c) **Polling Time Interval Entity**

Description: This entity describes the polling time interval (PTI) used for polling. The PTI is used by the **Initiate Polling** and **Calculate Polling Time Interval** activities, described in the Functional Model. The PTI is also used by relationships that define analysis rules, described in section 6.4.2.

Source: [GTE93b]

d) **Health Index Entity***

Description: This entity defines a health index value produced by the **Compute Health Index** activity, described in the Functional Model.

Parameterization: Selection of **Compute Fault "Health Index"** Optional operational feature.

Source: [GTE93b]

6.4.2 Description of Relationship Types

This section describes the relationships needed to specify event profiles and analysis rules. Three types of relationships are described. Part A describes Construct Pattern relationships. These relationships between individual Construct Pattern entities are needed to describe negation (not), conjunction (and), and disjunction (or) clauses of production rules. These relationships represent conditions and conclusions of event profiles and analysis rules. Part B describes Event Profile Constructs used for filtering. Part C describes relationships between

construct patterns that permit definition of analysis rules, including polling analysis, correlation, and alarm disposition rules. These relationships are shown in figures below.

6.4.2.1 Construct Pattern Relationships

Description: Construct Pattern relationships are combinations of **Construct Patterns** (described in sec. 6.4.1.1). These relationships are defined as unary relationships; that is--they have one role. Construct Pattern relationships are used in antecedents and consequents of analysis rules (described in sec. 6.4.2.3 below).

Source: [GENES92]

a) **Negation**

Description: This relationship denotes a negated (or not) condition in an analysis rule. That is, the condition represents a fact that should not be true for the rule to apply. The role **Negations** denotes the pattern that constitutes the negated (or not) clause.

unary Negation
Negations: (1) Construct Pattern or Conjunction

b) **Conjunction**

Description: The relationship denotes a conjunction of conditions (an "and" phrase) in which each condition satisfied for the rule to be true. The role **Conjuncts** refers to a combination of construct patterns, negations, or disjunctions (described below) that form conjunction of conditions.

unary Conjunction
Conjuncts: (M) Construct Patterns, Negations, Disjunctions

c) **Disjunction**

Description: The relationship denotes a disjunction of conditions (an "or" phrase), in which one condition must be satisfied to trigger the rule. The role **disjuncts** denotes construct patterns, negations, or conjunctions representing individual conditions of the disjunction.

unary Disjunction
Disjuncts: (M) Construct Patterns, Negations, or Conjunctions

6.4.2.2 Event Profile

Description: This relationship describes an event profile. An event profile matches incoming event notification. A matching notification may be reported to an external destination in the network, may be filtered out, or may be forwarded to the **Analyze Events** activity for further analysis. There are three roles in the relationship. **Notification Pattern** denotes a construct pattern that will match incoming event notifications. **Time of Operation** denotes the Schedule entity that describes when the event profile is to be in operation. **Forwarding destination** is an optional role for event profiles that forward alarm notifications to external network destinations. The role denotes the Communicating Entities to which an alarm notification should be forwarded. This relationship appears in figure 6.3.

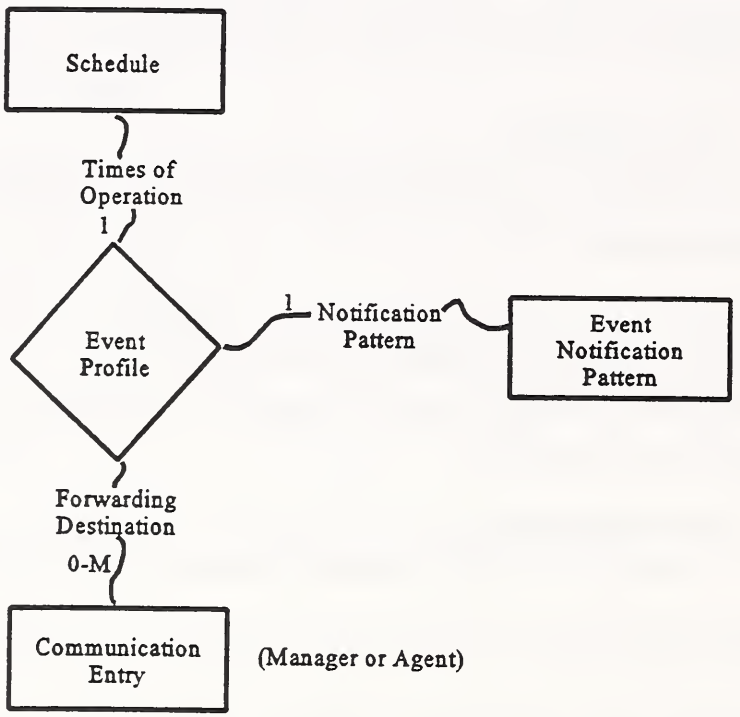


Figure 6.3: Details of Event Profile Relationship

Relationship Attributes: Result is an attribute that describes what happens when an event notification matches the event profile. As indicated above, possible results may be to report an alarm notification, filter the notification out or discard it, or forward the notification to Analyze Events. **Operational state** indicates whether the event profile is enabled or disabled.

3-ary Event Profile

Notification Pattern:	(1) Event Notification Pattern
Times of operation:	(1) Schedule
Forwarding destination:	(0-M) Communicating Entity

Source: [ISO/IEC 10165-5]

6.4.2.3 Analysis Rule

Description: This relationship represents the combination of construct patterns needed to specify an analysis rule. The relationship is specialized into relationships for Correlation Rule, Disposition Rule, and Polling Analysis Rule. Individual specializations retain the roles defined for Analysis Rule and may supply additional roles. Analysis rule has three roles. **Premise** refers to a single **Construct Pattern** or a **Conjunction**, **Disjunction**, or **Negation** relationship. **Consequent** refers to a **Construct Pattern** or to a **Conjunction** that is concluded if the premise is matched. **Time of operation** is an optional role that refers to a Schedule entity that indicates when the rule is operating.

Relationship Attributes: The **Operational state** attribute indicates whether or not the rule may be used. This attribute may have the values "Enabled" or "Disabled."

3-ary Analysis Rule

Premise:	(1) Construct Pattern, Conjunction, Disjunction, or Negation
Consequent:	(0-1) Construct Pattern or Conjunction
Times of Operation:	(1) Schedule

Source: [GTE93b], [GENES92], and [GOLD93]

a) **Correlation Rule**

Description: This specialization of analysis rule is used to assert correlations. The **premise** is constrained to refer to conjunction (as well as disjunction and negation) relationships consisting of construct patterns that represent a meaningful correlation of events occurring on a network resource or set of resources. This includes event notification patterns, network resource patterns, patterns for previous correlations, and functional expression patterns. The consequent role is constrained to refer to patterns for a **correlation assertion**. If the patterns in the premise part of the rule are matched, the consequent part--a correlation assertion--is asserted. That is, an instance of Correlation Assertion is created. The Correlation Rule relationship appears in figure 6.4.

3-ary Correlation Rule

Premise:	Constrained to (1) conjunction relationship or (M) disjunctions and negation relationships, consisting of patterns for network resources, event notifications, previous correlation assertions, and function patterns. (Disjunction and negation relationships are not shown in fig. 6.4.)
Consequent:	Constrained to instantiating patterns for (1) **Correlation Assertion**.
Times of Operation:	As above.

Additional Specialization: The expertise of local network administrators and network management experts will be used to define correlation rules for a particular alarm surveillance system.

Source: [GTE93b], [GENES92], and [GOLD93]

b) **Disposition Rule**

Description: This specialization of analysis rule is used to determine alarm dispositions. The premise role is constrained to conjunction, disjunction, or negation relationships consisting of patterns for alarm notification entities, **Correlation Assertions** concluded by a correlation rule, or to **Manager Inquiry Responses** that represent responses to follow-up manager inquiries. The consequent role is constrained to refer one or more specializations of **Manager Transmission** relationships (including its specialization--the **Alarm Disposition Report Transmission** relationship--described in sec. 6.3.2.2 and shown in figs. 6.1 and 6.2). Depending on the participation set of **Manager Transmission** (or **Alarm Disposition Report** relationship), the **message** role will refer to a pattern for either an alarm notification entity, a GET-type manager inquiry, or a change-in-operability state notification entity. For the alarm notification entity participation set of the manager report, the **disposition** attribute of this relationship may be used to identify whether the alarm is being cleared, reported, "held," or if its disposition is unknown. If the premise part of the rule is matched, the patterns referred to in the **message** role of the **Manager Report** relationship (or its **Alarm Disposition Report** specialization) are instantiated and the corresponding actions taken. This relationship appears in figure 6.4.

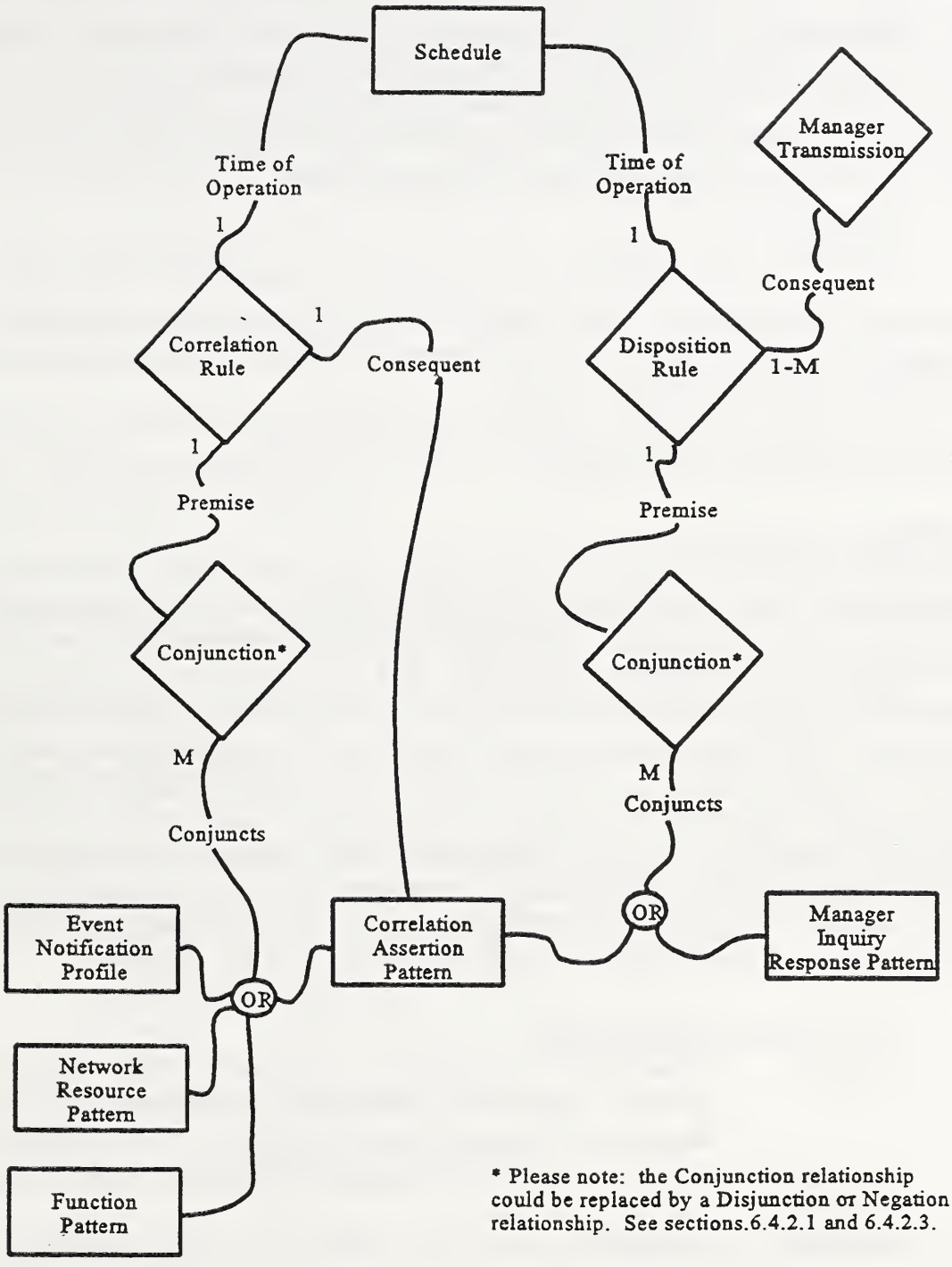


Figure 6.4: Correlation Rule and Disposition Rule

3-ary Disposition Rule

Premise:	Constrained to (1) conjunction or disjunction relationship consisting of patterns for **Correlation Assertion** or **Manager Inquiry Response**. (Only conjunctions are shown in fig. 6.4).
Consequent:	Constrained to refer to 1 or more **Manager Transmission** relationships (including **Alarm Disposition Report** specialization) for which the **message** role refers to a pattern for either an Alarm notification entity, a GET-type manager inquiry, or a change-in-operability state notification entity.
Times of Operation:	As above.

Additional Specialization: The expertise of local network administrators and network management experts will be used to define specific disposition rules that are relevant to a particular alarm surveillance system.

Source: [GTE93b] and [GENES92]

c) **Polling Analysis Rule**

Description: Polling analysis rules are used to identify agents that do not respond to poll messages and to issue **alarm notifications**. The **premise** role of this type of rule refers to a **Conjunction** or negation relationship that may consist of (1) a set of **network resources** being polled, (2) poll responses for the polled resources (either PING-type poll responses or GET-type manager inquiry responses), (3) a **polling time interval** entity, and (4) **Function Pattern** that, using the polling time interval, calculates the length of time that must elapse without receiving a poll response in order to issue an alarm. The **consequent** specifies an **alarm notification entity** pattern that, when instantiated, produces an appropriate alarm message. For more information on polling analysis, see the description of the **Analyze Poll Responses** activity provided in section 5.2.5.1 of this report. Polling analysis rules are currently not shown in the diagrams.

3-ary Polling Analysis Rule

Premise:	Constrained to conjunction relationships for (1-M) patterns for **network resources**, **polling time intervals**, **PING-type Poll Response**, **Manager Inquiry Response**, and **Function Patterns**.
Consequent:	Constrained to refer to patterns for **alarm notification entities**.
Times of Operation:	As above.

Additional Specialization: The expertise of local network administrators and network management experts will be used to define specific disposition rules that are relevant to a particular alarm surveillance system.

Source: [GTE93b] and [GENES92]

6.4.2.4 Construct Set*

Description: This relationship defines a set of event profiles or analysis rules that are used together. All of the members of a **Construct Set** are either enabled--that is operational--or disabled--not operational. The relationship has two roles. **Members** specifies the event profiles or analysis rules that belong to the construct set. **Times of Operation** is an optional role that refers to a **Schedule** entity. The **Schedule** entity describes when the construct set is operational.

binary Construct Set
Members: (M) Event Profiles or Analysis Rules
Times of
Operation: (1) Schedule

Attributes: The attribute **operational state** indicates whether the construct set is enabled or disabled. **Mode** is a parameterized attribute that describes the operating mode or modes for which the construct set is applicable.

Parameterization: The relationship is parameterized optional features for controlling filtering and analysis constructs. The attribute **Mode** is parameterized by the selection of the **Dynamic Surveillance Control** optional operating feature.

Source: [GTE93b]

a) **Event Profile Set***

Description: This is a specialization of **Construct Set** relationship for event profiles. The **Members** role is constrained to **Event Profiles. Times of Operation** is inherited from **Construct Set.** This relationship appears in figure 6.5.

binary Event Profile Set
Members: (M) Constrained to Event Profiles
Times of
Operation: As in **Construct Set.**

Attributes: Inherited from **Construct Set.**

Parameterization: This entity is parameterized by selection of the optional **Event Profile Sets** feature.

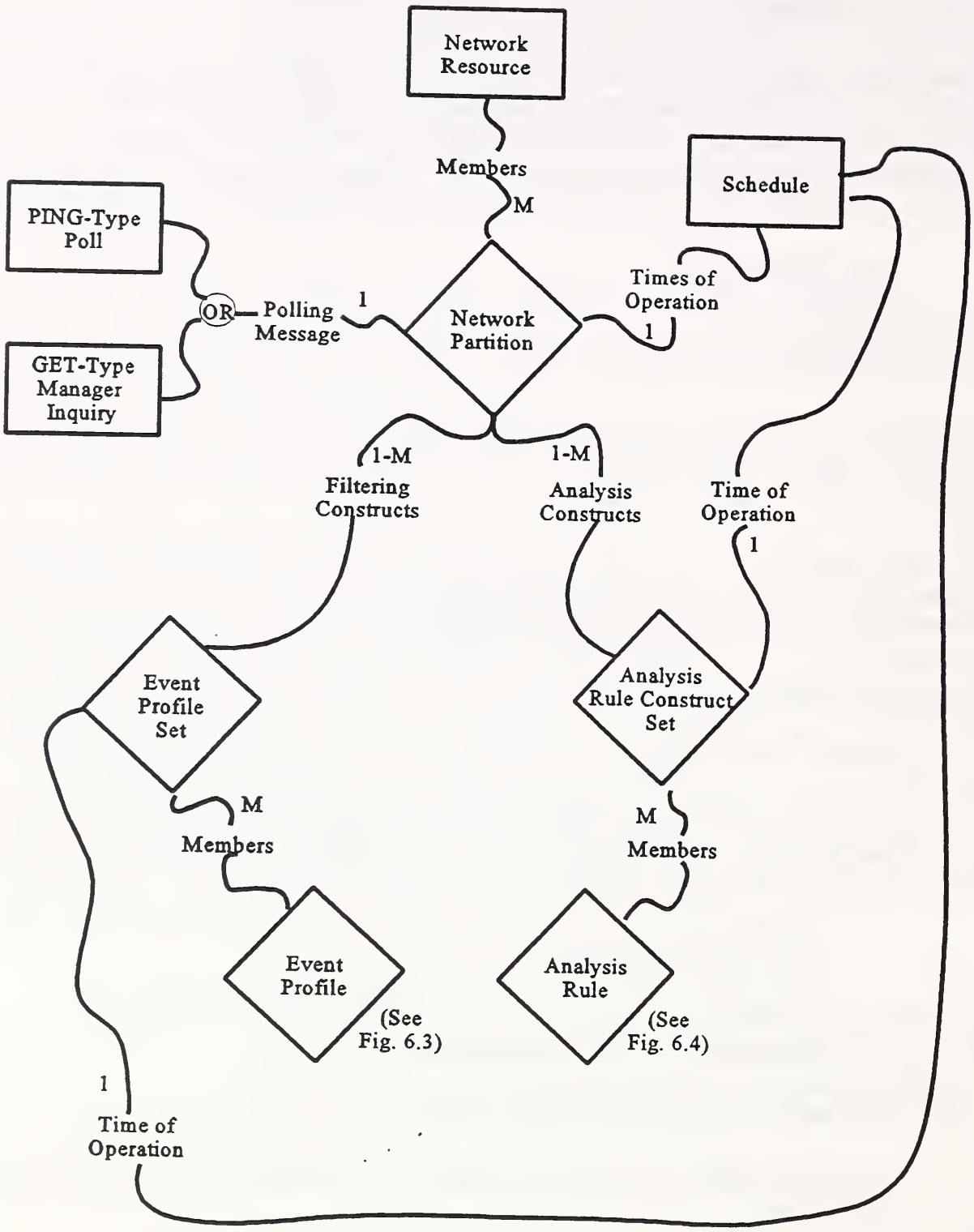


Figure 6.5: Construct Sets and Network Partitions

b) **Analysis Construct Set***

Description: This is a specialization of **Construct Set** relationship for analysis rules. The **Members** role is constrained to **Analysis Rules**. **Time of Operation** is inherited from **Construct Set**. This relationship appears in figure 6.5.

binary Analysis Construct Set
Members: (M) Constrained to Analysis Rules
Times of
Operation: As in **Construct Set**.

Attributes: Inherited from **Construct Set**.

Parameterization: This entity is parameterized by selection of the optional **Analysis Construct Set Control** feature.

6.4.2.5 Network Partition*

Description: This relationship describes a set of network resources that are monitored together. The relationship has two roles. **Members** specifies the network resources that belong to the partition. **Times of Operation** is an optional role that refers to a **Schedule** entity. The **Schedule** entity describes when the construct set is operational. The optional role **analysis constructs** specifies an **Analysis Rule Construct Set** relationships that are specially associated with this partition. This relationship appears in figure 6.5.

3-ary Network Partition

Members:	(M) Network Resources
Times of operation:	(1) Schedule
Analysis constructs:	(1-M) Analysis Construct Sets
Filtering constructs:	(1-M) Event Profile Set
Polling message:	(1) PING-type poll or GET-type Manager Inquiry

Attributes: The attribute **operational state** indicates whether the network partition is enabled or disabled for monitoring. **Mode** is a parameterized attribute that describes the operating mode or modes for which the construct set is applicable.

Parameterization: This relationship is parameterized by the selection of the **Partitioned Monitoring Organization** alternative feature. The entity is needed to support capabilities specified by the **Dynamic Surveillance Control** optional operational feature. The parameterization of **Mode** is dependent upon the selection of the **Dynamic Surveillance Control** optional operating feature.

6.4.2.6 Miscellaneous Relationships

This section contains miscellaneous relationships necessary to describe information structures that carry out analysis.

a) **Poll Response**

Description: This is the relationship between polls and poll responses corresponding to the data flow **match results**. There are two roles. **Poll** describes the poll messages that was sent. **Response** indicates the response, if there is one.

binary poll response

poll:	(1)	PING-Type Poll or GET-Type Manager Inquiry
response:	(0-1)	PING-Type Poll Response or Manager Inquiry Response

b) **Response Statistic Structure**

Description: This relationship describes the structure of polling response statistics. There are two roles. The **monitored resource** role, indicating the network resource to be monitored, is played by the **network resource** entity. The **time interval** role, which represents the time interval over which polling responses are accumulated, is played by the **polling time interval** entity. One relationship attribute is used to count the number of responses occurring over the time interval.

binary Response Statistic Structure:

Monitored resource:	(1) Network Resource
Time interval:	(1) Polling Time Interval

Relationship attribute: number of responses

6.5 Managed Resource and Network Configuration Structures

This section contains entities and relationships that describe network resources, their characteristics, and their interconnectivity. Information about network resources and connectivity is used to monitor the network, to update the network configuration to reflect the effects of fault reported in alarms, and to correlate alarms occurring on related resources. During correlation, specific elements of the network configuration may be retrieved to be matched by correlation rules. (Correlation rules are described in sec. 6.4.2.3). The entities and relationships in this section are summarized in figure 6.6.

6.5.1 Description of Entity Types

Three types of entities are described: site, network, and network resource. The subtyping of the entity, network resource, is extensive. Relationships specify containment and connectivity relationships between network resources.

6.5.1.1 Subnetwork

Description: Generally, a network is a set of devices such as computers, terminals, and printers that are physically connected by a transmission medium so that they can communicate with each other. Networks can also be viewed as logical units that belong to a particular organization or to a unit within the organization.

Attributes: Attributes are used to hold information relevant to the context features, including **network type** (LAN, MAN, or WAN) and **bandwidth.**

Source: [NMF92] and [GTE93b]

6.5.1.2 Network Resource

Description: An element of a communications network that is managed, or in this case, monitored by an alarm surveillance system. A network resource may include a network device or a communications service.

Attributes: The following variables are based on the ISO/IEC Alarm Reporting Function standards profile [ISO/IEC 10164-4]. **Operability state** describes whether the network resource is currently enabled or disabled. **Procedural status** indicates whether external initialization is required, the device is in the process of initializing, or the device is reporting. **Standby status** indicates whether the device is on "hot standby," "cold standby," or "providing service." **Alarm status** indicates if a reported fault or problem is ranked as critical, major, or minor. **Degraded** describes if the operation of the resource has been degraded. **Repair status** indicates if the resource is not under repair, is being repaired, or is in test. **Resource criticality level** indicates the level of criticality of the resource in meeting the operational objectives of the network. The OSI attributes **back up resources** and **dependency** are represented in this domain model as relationships.

Source: [ISO/IEC 10164-4], [ROSE91], and [TANEN88]

a) **Network Device**

Description: This entity refers to any device that is part of and can send or receive digital electronic transmissions across a **network**. Network devices are described in section 2.1.3 of the A Context Analysis of the Network Management Domain [DABR93].

Attributes: The attribute **usage state** indicates if the device is idle, active, or busy.

a.1) **End-system Device**

Description: A platform containing hardware and possibly software systems that utilize the communications services provided on the network. End users of the communications network may utilize end-system devices to run applications. Alternatively, application system may run on end-system devices without user intervention.

Additional Specialization: The entity may be specialized for different types and makes of devices. The specializations are numerous and reflect specific makes and versions of commercial products.

a.2) **Intermediary Device**

Description: A network device that influences the transmission path in some way. Typically, intermediary devices are network devices that connect different subcomponents of the network such as bridges, routers, and gateways.

Additional Specialization: The entity may be specialized for different types and makes of devices. The specializations are numerous and reflect specific makes and versions of commercial products.

a.3) **Link Device**

Description: A network device that consists of, or includes, transmission media that propagates digital signals.

Attributes: **Bandwidth** is an important attribute of link devices.

Additional Specialization: The entity may be specialized for different types and makes of devices. The specializations are numerous and reflect specific makes and versions of commercial products.

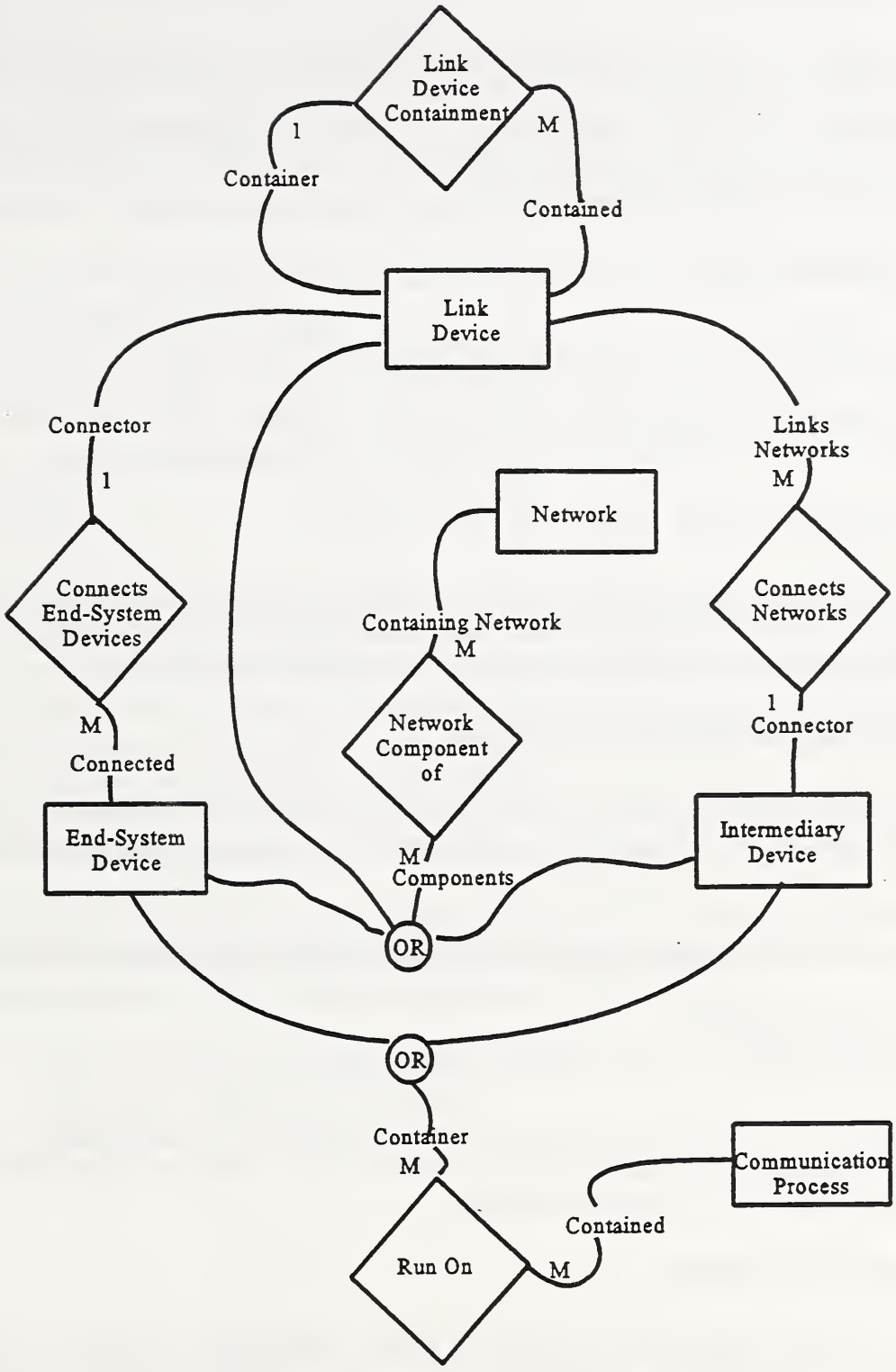


Figure 6.6: Containment and Connection Relationships

b) **Managed Process**

Description: A communications process initiated and controlled by an Automated Processing Capability; i.e., one or more specific hardware, firmware, or software components. At present management of processes is uncommon and is generally not a requirement for alarm surveillance application systems. However, two types of potential managed processes are described.

b.1) **Dynamic Link**

Description: A process or set of processes that enable a connection between two network devices (usually End-system Devices) used to transfer data. A dynamic link may encompass many Link Devices (Static Links). Dynamic links use connection-oriented protocols and are terminated when the data transfer is ended.

b.2) **Communications Process**

Description: A process that enacts some aspect of transmission between devices across a network. Typically, the process performs a specific function called for by a protocol within a protocol layer of a suite of protocols such as Internet or OSI.

6.5.2 Description of Relationship Types

These relationships describe the kinds of links between entities defined in the preceding section. All relationships are based on a single general relationship **Resource Link**, described below:

Description: This the generic category of relationships that exist between resources.

unary Resource Link:
Linked Resources: (1-M) Network Resource

Major categories of relationships include resource containment relationships and resource connection relationships. These are shown in figure 6.1. Selected specializations of these relationships are depicted in figure 6.6 below.

6.5.2.1 Agent Responsibility

Description: Agent Responsibility denotes a binary relationship between an agent and the managed resource the agent is responsible for. The role **agent for** denotes the agent. The role **managed resource** denotes one or more network resource entities, the agent is responsible for. Network Resource entity is describe in section 6.5.1.2. The relationship is shown in figure 6.1.

Source: [GTE93a], [ISO/IEC 10165-2], [ROSE90a], and [ROSE91]

binary Agent Responsibility:
Agent for: (1) Agent
Managed Resource: (M) Network Resource

6.5.2.2 Resource Containment

The generic **resource containment** relationship is defined below.

Description: The roles **container** and **contains** both refer to any kinds of network resources. The cardinality is set to many to many.

Source: [NMF92]

binary Resource Containment
Container: (M) Link Device
Contained: (M) Link Device

Four specializations of the resource containment relationship are defined: **network component of** which associates network resources with the networks they are members of; **Runs On** which describes communications processes that are contained by the devices they run on; **Link Device Containment** which refers to physical containing relationships that occur among link devices and intermediary devices on the network; and **Dynamic Link Containment** which refers to connections established across devices on the network.

a) **Network Component Of**

Description: This is a binary relationship between a network and network resources. The role **containing network** denotes the network; **components** denotes one to many network resources. This relationship is shown in figure 6.6.

binary Network Component Of:
Containing network: (1) Network
Components: (M) Network Resource

b) **Runs On**

Description: This relationship refers to a communications process that runs on a network device. The role **contained** refers to the **Communications Process** entity. The role **container** refers to the end-system or intermediary device that the process runs on. The cardinality of the relationship is many to many. This relationship is shown in figure 6.6.

binary Runs on:

Container:	(M) End-System Device or Intermediary Device
Contained:	(M) Communications Process

c) **Link Device Containment**

Description: This relationship describes physical containment between link devices: that is, one physical link which is spanned by on or more other physical links. The roles **container** refers to **link device** entities. **Contains** may refer to **link device** entities as well as **intermediary device** entities that connect link devices. The relationship is shown in figure 6.6.

binary Link Device Containment

Container:	(1) Link Device
Contained:	(M) Link Device or Intermediary Device

d) **Dynamic Link Containment**

Description: This relationship describes physical containment by dynamic links of the physical links they span. The role **container** refers to a **Dynamic Link** entity, and role **contains** refers to a **Network Device** entity. (Dynamic links span all three types of network devices.) The relationship has a many to many cardinality. This relationship is omitted from the figures.

binary Dynamic Link Containment

Container:	(M) Network Device
Contained:	(M) Dynamic Link

6.5.2.3 Resource Connection

Description: Resource connection relationships describe links between network resources. These links are considered essential to describing connectivity between network resources for the purpose of correlating alarm notifications. These relationships are shown in figure 6.6.

Source: [NMF92]

a) **Connects End-System Devices**

Description: This relationship captures the connection between the link device that connects one or more end-system devices. The role **connector** refers to the link device. The role **connected** refers to the end-system device.

binary Connects end-system devices:
Connector: (1) Link Device
Connected: (M) End-System Device

b) **Connects Networks** (Subnetworks)

Description: This relationship captures the connection between two separate networks. The connection is enabled by an intermediary device that connects two or more network devices belonging to different networks. The role **connector** refers to the intermediary device. The role **connected** refers to the end-system device. The role **Connected links** refers to either link devices (or possibly end-system devices) belonging to different networks (subnetworks).

binary Connects networks:

Connector:	(1) Intermediary Device
Links networks:	(M) Link Devices (belonging to different subnetworks)

7. REFERENCES

[ADAMS91] Adams, E., "Global Commonality in User Requirements," in Integrated Network Management, II: Proceedings of the IFIP TC6/WG6.6 Second International Symposium on Integrated Network Management, I. Krishnan and W. Zimmer (eds.) held Washington, DC, April 1-5, 1991, pp. 171-181, Elseveir Science Publishers, Amsterdam, Netherlands.

[ASTEC90] A User's Manual for CaMERA, A Culture-adaptive Mechanism for Expression, Reflection, and Analysis, Advanced Systems Technology Corporation (ASTEC), Crofton, MD, 1990.

[CASE90] Case, J., et al., A Simple Network Management Protocol, Request for Comments 1157, DDN Network Information Center, SRI International, May 1990.

[COHEN92] Cohen S., J. Stanley, S. Peterson, and R. Krut, Application of Feature-Oriented Domain Analysis to the Army Movement Control Domain, CMU/SEI-91-TR-28, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA, 1992.

[COMER91] Comer, Douglas E., Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture, Second Edition, 1991, Prentice-Hall, Inc., Englewood Cliffs, NJ 07632.

[DABR93a] Dabrowski, C. and T. Kirkendall, Preliminary Report on Domain Analysis Methods, Produced for the Software Producibility MODIL, National Institute of Standards and Technology, Gaithersburg, MD, February 1993.

[DISA93] Domain Analysis and Design Process, Version 1, The Defense Information Systems Agency, Center for Information Management, Software Reuse Program, Document No. 1222-04-210/30.1, March 30, 1993.

[DoD88] MILITARY STANDARD, Defense System Software Development, DOD-STD-2167a, Department of Defense, February 28, 1988.

[GOLD93] Goldszmidt, G. and Y. Yemini, "Evaluating Management Decisions via Delegation," Integrated Network Management, Volume 3, Number 12, 1993, pp. 247-257.

[GTE93a] Knowledge Acquisition Sessions With Domain Experts from GTE Government Systems at Chantilly, VA, Chantilly, VA, April-June, 1993.

[GTE93b] Knowledge Acquisition Sessions With Domain Experts from GTE Government Systems at Chantilly, VA, Chantilly, VA, from September 1993 until March 1994.

[GTE93c] Knowledge Acquisition Sessions With Domain Experts from GTE Government Systems at Needham, MS, Telephonic sessions, May, 1994.

[HOLI91] Holibaugh, R., "Joint Integrated Avionics Working Group (JIAWG) Object-Oriented Domain Analysis Method (JODA)--DRAFT DOCUMENT," Revision Number 3.1, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA, January 1991.

[ISO/IEC 9595] International Organization for Standardization, "Information Technology - Open Systems Interconnection - Common management information service definition [for CCITT Applications]," ISO JTC1/SC21, 1990.

[ISO/IEC 9596-1] International Organization for Standardization, "Information Technology - Open Systems Interconnection - Common Management Information Protocol - Part 1: Specification," ISO JTC1/SC21, 1990.

[ISO/IEC 10164-4] International Organization for Standardization, "Information Technology - Open Systems Interconnection - Systems Management - Part 4: Alarm Management," ISO JTC1/SC21, 1991.

[ISO/IEC 10164-5] International Organization for Standardization, "Information Technology - Open Systems Interconnection - Systems Management - Part 5: Event Report Management Function," ISO JTC1/SC21, 1991.

[ISO/IEC 10164-6] International Organization for Standardization, "Information Technology - Open Systems Interconnection - Systems Management - Part 6: Log Control Function," ISO JTC1/SC21, 1991.

[KANG90] Kang, K., S. Cohen, J. Hess, W. Novak, and S. Peterson, Feature-Oriented Domain Analysis (FODA) Feasibility Study, CMU/SEI-90-TR-21, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA, 1990.

[KATZ93] Katz, S., C. Dabrowski, and M. Law, Glossary of Reuse Terms, Draft Produced for the Software Producibility MODIL, National Institute of Standards and Technology, Gaithersburg, MD, July 1993,

[NMF92a] Network Management Forum, "Reconfigurable Circuit Service: Configuration Management Ensemble," OMNIPoint Specifications and Technical Reports, Book I and II, August 1992.

[NMF92b] Network Management Forum, "Reconfigurable Circuit Service: Alarm Surveillance Ensemble," OMNIPoint Specifications and Technical Reports, Book I and II, August 1992.

[NMF92c] Network Management Forum, "Application Services: Path Tracing Function," OMNIPoint Specifications and Technical Reports, Book I and II, August 1992.

[NMF92d] Network Management Forum, Statement of User Requirements for Management of Networked Information Systems, October 1992.

[NMF92e] Network Management Forum, "Reconfigurable Circuit Service: Configuration Management Ensemble," OMNIPoint Specifications and Technical Reports, Book I and II, August 1992.

[PETE91] Peterson S., and S. Cohen, A Context Analysis of the Movement Control Domain for the Army Tactical Command and Control System (ATCCS), CMU/SEI-91-SR-3, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA, 1991.

[PRIE90] Prieto-Diaz, Ruben, "Domain Analysis: An Introduction," ACM SIGSOFT Software Engineering Notes, Vol. 15, No. 2, April 1990, pp. 47-54.

[PRIE91] Prieto-Diaz, R., The Reuse Library Process Model, IS-40.2 03041-002, STARS Reuse Library Program, New York, March 1991.

[ROSE90a] Rose, M. (ed.), Management Information Base Network Management of TCP/IP based Internets: MIB-II, Request for Comments 1158, DDN Network Information Center, SRI International, May 1990.

[ROSE90b] Rose, M. and K. McCloghrie, Structure and Identification of Management Information for TCP/IP based Internets, Request for Comments 1155, DDN Network Information Center, SRI International, May 1990.

[ROSE91] Rose, M. The Simple Book: An Introduction to Management of TCP/IP-based Internets, Prentice-Hall, Inc., Englewood Cliffs NJ, 1991.

[SPC92] Domain Engineering Guidebook, SPC-92019-CMC, version 01.00.03, Software Productivity Consortium, Herndon, VA, December 1992.

[STAL88] Stallings, W., Data and Computer Communications, (second edition), Macmillan Publishing Company, New York, NY, 1988.

[STAL93] Stallings, W., Networking Standards: A Guide to OSI, ISDN, LAN, and MAN Standards, Addison-Wesley, Reading, MA, 1993.

[TANEN88] Tanenbaum, A., Computer Networks, Prentice-Hall, Englewood Cliffs, NJ, 1988.

[WART92] Wartik, S. and R. Prieto-Diaz, "Criteria for Comparing Reuse-Oriented Domain Analysis Approaches," International Journal of Software Engineering and Knowledge Engineering, Volume 2, Number 3, pp. 403-431, September 1992.

APPENDIX A: DOMAIN DICTIONARY

A dictionary of major terms and concepts is presented. Within individual definitions, terms in bold print are defined as separate entries. Sources for definitions are cited in brackets. The use of the notation "+ed" indicates that the original definition has been edited. The notation "(NIST)" indicates that definition was developed by the Domain Analysis Case Study team.

A.1 General Terms

This section provides terms, defined during the context analysis phase, that are important for understanding the domain model.

Accounting Management:
The collecting and storing of information about the utilization of **network resources** for purposes of generating bills for **end users** and/or end-user groups. [NMF92c] +ed

Agent:
A software system residing on a managed device that is responsible for carrying out **network management** functions on the device, including the execution of **management operations** initiated by the **manager**. [FIPS179], (NIST)

Alarm:
A particular type of **notification** that conveys information about a detected **fault**. An alarm may include information about the type of fault that has been detected, information about the circumstances surrounding the fault, and an estimate of the severity of the fault. [ISO/IEC 10164-4] +ed

Alarm Analysis:
The process of **alarm filtering**, **alarm correlation**, and routing of filtered and correlated alarms. See Alarm Filtering and Alarm Correlation. [GTE93], (NIST)

Alarm Correlation:
The process of comparing information in different **alarms** to determine if they arose from the same, or related, **faults** or **fault conditions**. [GTE93], [NMF92b] +ed

Alarm Filtering:
The process of controlling the flow of **alarms** and other **notifications** describing events that have occurred to ensure that (1) the resources of **network management** are directed to the **faults** whose resolution is necessary to effectively manage the **network** and (2) network performance is not degraded through transmission of redundant or useless information. Filtering includes using **discrimination criteria** to select alarms to be forwarded and to select alarms to be discarded. Filtering also includes determining the destination to which alarms should be forwarded. [GTE93], [ISO/IEC 10164-5] +ed

Alarm Management:
See Alarm Surveillance.

Alarm Reporting:
An OSI term that refers to the communication of information about a possible detected **fault**. This information generally includes the identification of the **network device** or **network resource** in which the fault was detected, the type of the fault, its severity, and its probable cause. The fault is reported in a **notification** called an **alarm**. See Alarm and Fault Detection. [ISO/IEC 10164-4] +ed

Alarm Surveillance:
The set of functions that enable (1) the monitoring of the **communications network** to detect **faults** and fault-related events or conditions, (2) the logging of this information for future use in **fault detection** and other **network management** activities, and (3) the analysis and control of **alarms**, **notifications**, and other information about faults to ensure that the resources of network management are directed toward faults that affect the operation of the communications network. Analysis of alarms consists of **alarm filtering**, **alarm correlation**, and **fault prediction**. [NMF92b], [GTE93] +ed

Alert:
See Alarm.

Bandwidth:
The rate at which information can be transmitted in bits/second. (NIST)

Centralized Network Management Architecture:
A **network management architecture** in which one **manager** at a single location controls the entire **communications network**. See Network Management Architecture, Distributed Network Management Architecture, and Distributed Hierarchical Network Management Architecture. [GTE93] +ed

CMIP:
See Common Management Information Protocol.

CMIS:
See Common Management Information Service.

Common Management Information Protocol (CMIP):
A **network management protocol** that supports the basic services defined in **Common Management Information Service (CMIS)** by specifying lower-level data units for transmitting CMIS operations and **notifications**. CMIP is described in [ISO/IEC 9596-1]. See Common Management Information Service (CMIS).

Common Management Information Service (CMIS):

A **network management protocol** that defines a set of basic network management services used by **network management systems** in the **Open Systems Interconnection** suite of protocols. CMIS includes but is not limited to **management operations**, called management-operations services, that are initiated by **managers**. It also includes **notifications** that can be sent by **agents**, referred to as management-notification services. CMIS is described in [ISO/IEC 9595].

Communications Network:

A system consisting of a **network** and a set of **communications services** that enable transmissions (voice, data, or other forms) to take place between persons, software applications, or other equipment. The users of the communications network are called **end users**. (NIST)

Communications Services:

The set of capabilities provided by software systems and **network devices** that enable transmissions from one point to another in the **network**. (NIST)

Configuration Database:

A database describing **network configurations**. The database may include a history of changes made to the network configuration. (NIST)

Configuration Management:

As used in **network management**, the tracking and control of the **network resources** and their current and potential connections. Configuration management includes creating and maintaining an accurate inventory of:

- the resources associated with the **communications network**,
- each network resource's operating characteristics--described by values of specific internal settings or variables,
- each network resource's logical and physical connections to other resources, and
- the **network topology** or any portion of it.

Configuration management controls the **network configuration**. It provides the means to change the operating characteristics of individual network resources, the logical and physical connections of resources, and the network topology. [NMF92e] +ed

Discrimination Criteria:

In **alarm filtering**, the criteria used to select whether or not to forward or discard an **alarm** or **trap**. See Alarm Filtering. [ISO/IEC 10164-5] +ed

Distributed Hierarchical Network Management Architecture:

A **network management architecture** with multiple levels of **manager** software systems in which (1) different managers have responsibility for different parts of the **communications network** and (2) higher-level managers control lower-level managers. See Network Management Architecture, Centralized Network Management Architecture, and Distributed Network Management Architecture. [GTE93] +ed

Distributed Network Management Architecture:

A **network management architecture** in which different **manager** software systems have responsibility for different parts of the **communications network**. In a distributed architecture, managers are said to be in a "peer to peer" relationship with respect to each other and do not control each other. See Network Management Architecture, Centralized Network Management Architecture, and Distributed Hierarchical Network Management Architecture. [GTE93] +ed

End-System Device:

A platform containing hardware and possibly software systems that utilize the **communications services** provided on the **communications network**. (NIST)

End User:

The user of the services provided by a **communications network**. A user may be a person or a software application. (NIST)

Error:

The deviation of a system from normal operation that may have been caused by a **fault**. [ISO/IEC 10164-4]

Fault:

A physical malfunction or abnormal pattern of behavior that is causing or will cause, an **outage**, **error**, or degradation of **communications services** on a **communications network**. [ISO/IEC 10164-4], [GTE93] +ed

Fault Condition:

A set of circumstances associated with a **network resource** or group of resources that is likely to lead to a **fault**. [GTE93] +ed

Fault Correction:

The corrective action(s) taken in response to a **fault** necessary to restore **communications services**. Corrective actions may include temporarily reconfiguring a portion of the **communications network** or repair of **network devices**. [NMF92c], [NMF92d] +ed

Fault Detection:

The process of discovering and reporting active **faults**, potential faults, and fault-related conditions. See Alarm Reporting. [NMF92d]

Fault Diagnosis:

The process by which (1) a detected **fault** is isolated or narrowed down to a specific **communications network** element in which the fault occurred and (2) additional information about the circumstances of the fault is obtained that will be needed for **fault correction**. See Fault Correction. [NMF92c] +ed

Fault Management:

The detection, reporting, diagnosis, correction, and prevention of **faults** and **fault conditions**. Fault management includes **alarm surveillance**, **trouble tracking**, **fault diagnosis**, and **fault correction**. [NMF92c] +ed

Fault Prediction:

The process of using current and historical information about **alarms** and other events to predict **faults** or to identify developing **fault conditions**. [GTE93] +ed

Fault Tracking:

See Trouble Tracking.

Intermediary Device:

A **network device** that influences the transmission path in some way. Typically, intermediary devices are network devices that connect different subcomponents of the **network**. Examples are bridges, routers, and gateways. (NIST)

Internet Suite of Protocols:

A suite of **protocols** that grew out of early research by the Advanced Research Projects Agency (ARPA) in DoD and has since spread to many areas on government and industry. The Internet suite is usually referred to as **TCP/IP (Transmission Control Protocol/Internet Protocol)**. (NIST)

LAN:

See Local Area Network.

Link Device:

A **network device** that consists of, or includes, a **transmission medium** that propagates digital signals. (NIST)

Local Area Network (LAN):

A **communications network** that is usually limited to a single building or closely-spaced group of buildings. (NIST)

MAN:

See Metropolitan Area Network.

Managed Network:

The set of all **network resources**, including **network devices** and **communications services**, that are subject to **network management** and that are controlled by a particular **network management system**. (A **communications network** may also contain network resources that are not subject to network management. These are not part of the managed network.) See Communications Network. See Managed Device. (NIST)

Management:

Generically, the monitoring and control of a set of resources, activities, or events. See Network Management. (NIST)

Management Application:

See Manager.

Management Information Base (MIB):

A standardized description of the information that must be maintained by managed devices responding to **network management protocols**. A MIB is implemented on a device as a collection of variables that can be used to describe and control the device's state. MIBs are described in [ROSE90a]. See Management Operation. [ROSE90a] +ed

Management Operation:

A low-level operation specified in a **network management protocol** that a **manager** can perform on a **network resource** in a **managed network**. A management operation may be a "GET" operation that obtains information from a network resource's **Management Information Base**. This information can be used to interpret the state of a managed device or other network resource. A management operation may also be a "SET" operation that alters variable settings in order to control the operating status or configuration of a managed device or other network resource. (NIST)

Management Station:

See Network Management Station.

Manager:

A major part of a **network management system**--a manager is a software system that initiates actions for monitoring and controlling a set of **network devices** or other **network resources**. The actions of a manager include but are not limited to initiating **management operations** that are carried out by **agent** systems residing on network devices. Such devices are referred to as managed devices. Managers also respond to **notifications** sent by agent systems describing the status of a managed device. See Agent, Managed Device, Managed Network, Management Operation, and Network Management System. [FIPS179] +ed

Metropolitan Area Network (MAN):

A **communications network** located in a single city or metropolitan area. A MAN may be composed of LANs or even other MANs. (NIST)

MIB:

See Management Information Base.

Monitoring Strategy:

The procedure for monitoring a **communications network** to detect **faults** and **fault conditions** and to determine the status of the network's managed devices and other **network resources**. A monitoring strategy may involve a procedure for periodically **polling** individual **managed devices** to determine their status, receiving **alarms** automatically transmitted by **agent** systems residing on the devices, or a combination of these methods. See Alarm and Polling. (NIST)

Network:

A set of devices such as computers, terminals, and printers that are physically connected by a **transmission medium** so that they can communicate with each other. These devices are called **network devices**. See Communications Network, Managed Network, and Network Device. (NIST)

Network Configuration:

A specific set of **network resources** that form a **communications network** at any given point in time, the operating characteristics of these network resources, and the physical and logical connections that have been defined between them. (NIST)

Network Control:

The initialization and shut down of **network resources**. (NIST)

Network Control Center:

See Network Operations Center.

Network Device:

A device that is part of and can send or receive electronic transmissions across a **communications network**. Network devices include: **end-system devices** such as computers, terminals, or printers; **intermediary devices** such as bridges and routers that connect different parts of the communications network; and **link devices** or transmission media. [ROSE91], [TANEN88] +ed

Network Management:

The discipline that describes how to monitor and control the **managed network** to ensure its operation and integrity and to ensure that **communications services** are provided in an efficient manner. As described in [ISO/IEC 7498-1], network management consists

of **fault management**, **configuration management**, **performance management**, **security management**, and **accounting management**. (NIST)

Network Management Architecture:
The distribution of responsibility for **management** of different parts of the **communications network** among different **manager** software systems. The network management architecture describes the organization of the management of a network. The three types of network management architectures are the **centralized network management architecture**, the **distributed network management architecture**, and the **distributed hierarchical network management architecture**. (NIST)

Network Management Protocol:
A **protocol** whose purpose is to convey information pertaining to the **management** of the **communications network**, including **management operations** from **managers** as well as responses to **polling** operations, **notifications**, and **alarms** from **agents**. [ROSE91] +ed

Network Management Station:
A computing platform on which the **manager** system runs. In addition to the manager, the station contains the workstations, displays, automatic data processing hardware and software, and ancillary equipment and facilities used to provide the ability to manage the **communications network**. (NIST)

Network Management System:
A software system that performs functions of **network management** for a **communications network**. This system may include both **manager** and **agent** systems. Since network management is not fully automated, a network management system performs a subset of network management functions as defined in [ISO/IEC 7498-1]. (NIST)

Network Operations Center:
An installation or site that contains the personnel, equipment, and other **network resources** needed to operate, control, and maintain the portion of the **communications network** within its jurisdiction. (NIST)

Network Resource:
An element of a **communications network** to be managed, including a **network device** or a **communications service**. [NMF92a] +ed

Network Size:
The total number of **network devices** that must be managed within the **network** and all its subcomponents. (NIST)

Network Topology:

The term has two meanings: (1) the structure, interconnectivity, and geographic layout of a group of **networks** forming a larger network and (2) the structure and layout of an individual network within a confined location or across a geographic area. (NIST)

Notification:

A message emitted by an **agent**. A notification may describe an event that has occurred within the managed device. [ISO/IEC 10040], [ISO/IEC 10164-4] +ed

Open System Interconnection (OSI) Suite of Protocols:

A suite of **protocols** developed under the auspices of the International Organization for Standardization/International Electrotechnical Committee (ISO/IEC). (NIST)

Outage:

The period of time for which a **communications service** is unavailable [ISO/IEC 10164-4].

Performance Management:

The process of monitoring and controlling a **communications network** to ensure that it operates efficiently. This function includes (1) the collection and evaluation of data that measures the efficiency of the communications network in meeting its operational objectives and (2) the controlled change of any factors to improve that efficiency. [NMF92c] +ed

Polling:

The process of sending messages to individual managed devices to determine their operational status. (NIST)

Proprietary Element Management System:

A software system intended to monitor and control a collection of **network devices** that respond to a **proprietary protocol**. Proprietary element management systems may be developed and supplied by commercial vendors. See Standards-Based Element Management System. [GTE93] +ed

Proprietary Protocol:

A **protocol, network management protocol**, or suite of protocols developed by a private company to manage **network resources** manufactured by that company. See Proprietary Element Management System. (NIST)

Protocol:

A formal description of message formats and rules that must be followed to exchange messages. Protocols can describe high-level exchanges between application programs (e.g., the way in which two programs transfer a file across an internet). Protocols may also describe low-level details of machine-to-machine interfaces (e.g., the order in which

the bits from a byte are sent across a wire). Most protocols include both intuitive descriptions of expected interactions as well as more formal specifications based on finite state machine models. [COMER92] +ed

Resource:
See Network Resource.

Scope:
The geographic area that a **network** spans. (NIST)

Security Management:
The process of monitoring and controlling access to **network resources**. This includes monitoring usage of network resources, recording information about usage of resources, detecting attempted or successful violations, and reporting such violations. [ISO/IEC 7498-4], [NMF92c] +ed

Simple Network Management Protocol (SNMP):
A **network management protocol** used with the **TCP/IP** suite of protocols. SNMP specifies a set of management operations for retrieving and altering information in a **Management Information Base** (MIB), authorization procedures for accessing MIB tables, and mappings to lower TCP/IP layers. An expanded version of SNMP is being created, called SNMPv2, that will provide additional services. SNMP is described in [CASE90] and [ROSE91].

Size:
See Network Size.

SNMP:
See Simple Network Management Protocol.

Standards-Based Element Management System:
A software system that monitors and controls a collection of **network devices** that respond to either the **Open System Interconnection (OSI) Suite of Protocols** or **TCP/IP (Transmission Control Protocol/Internet Protocol)**. Standards-based element management systems may be developed and supplied by commercial vendors. See Proprietary Element Management System. [GTE93] +ed

Systems Management:
See Enterprise Network Management.

TCP/IP (Transmission Control Protocol/Internet Protocol):
See Internet Suite of Protocols.

Topology:
See Network Topology.

Transmission Medium:
A mechanism that supports propagation of digital signals. Examples of a transmission medium are cables such as leased lines from common commercial carriers, fiber optic cables, and satellite channels. [TANEN88]

Trap:
A message indicating that a **fault condition** may exist or that a **fault** is likely to occur. See Alarm. [GTE93]

Trouble Tracking:
The process of recording, updating, maintaining, and forwarding information about the progress of a reported **fault** to support personnel or automated systems in order to ensure the fault is diagnosed and corrected in a timely manner. (NIST)

WAN:
See Wide Area Network.

Wide Area Networks (WAN):
A **communications network** that covers several sites that are geographically distant. A WAN may span different cities or even different continents. (NIST)

A.2 Functional Model Terms

This section defines terms that are relevant to the Functional Model. The term definitions include data flows and control flows. Appendix B.1 provides a table showing the correspondence between individual flows and specific entities and relationships. Appendix B.3.1 summarizes a hierarchy of data flow types; Appendix B.3.2 summarizes control flow types.

"Alarm Disposition Unknown" Message:
A report issued by an alarm surveillance system that indicates that the disposition of an **alarm notification** cannot be determined. The determination cannot be made because the **alarm surveillance** system does not "know" what to do; i.e., it lacks the appropriate **disposition rules**.

Alarm Notification:
An **event notification**, generally issued by an **agent** system, that conveys information about a perceived **fault** or fault-related condition.

Alarm Threshold Set Requests:

Requests initiated by a network administrator or automated source to change the threshold levels for **alarm notifications** issued by **agent** systems. Data describing alarm thresholds is stored in internal data structures maintained by agent systems at the site of the **network resources** being managed. The alarm surveillance system must issue a **alarm threshold update** to physically change the threshold value.

Alarm Threshold Update:

A request to update a data structure on a managed **network resource** that contains the value of an alarm threshold. It is assumed that the alarm threshold update is issued by an **alarm surveillance** system as a result of an **alarm threshold set request.**

"Alarm to Destination" Mappings:

A control flow that specifies where **reported alarms, cleared alarms,** and **"alarm disposition unknown" messages** should be sent.

Analysis Construct:

A data structure that can be used to control how analysis is performed by the **alarm surveillance** system. Analysis constructs can be either **analysis rules** or **analysis construct sets** that consist of groups of rules.

Analysis Construct Set:

A collection of **analysis rules** that are used together. A particular analysis construct set may be used when the **communications network** goes into a particular operating mode. An analysis construct set may also be applied to a particular network partition of monitored devices.

Analysis Construct Control:

A control flow that controls the operation of **analysis constructs** and **analysis construct sets.** Analysis construct control is a decomposition of **construct operation control.** Analysis construct control is specialized to individual analysis rule control and **analysis construct set control.**

Analysis Construct Set Control:

A control flow that controls the operation of **analysis constructs sets.** Analysis construct set control is a decomposition of **analysis construct control.**

Analysis Rule:

A rule or heuristic that determines how a particular analysis activity is carried out. Specific types of analysis rules are **correlation rules, polling analysis rules,** and **disposition rules.**

Binary Encoding Rules:

A language for describing the syntax of **messages** transferred across a network [ROSE91].

Change-in-State Notification:

An **event notification** that reports a change in the value of one or more internal variables that describe the state of a **network device**. A change-in-state notification may not necessarily convey information that is related to a **fault**. Compare with **alarm notification**. See event notification.

Cleared Alarm:

A previously reported alarm that has been determined to no longer present a problem. The clearing action may originate at the source of the problem and is emitted by an **agent** system. The clearing action may also be determined by the **alarm surveillance** system in the Determine Alarm Disposition activity using **disposition rules**.

Configuration Update:

A request to modify configuration information that is being maintained about the **network configuration**. The requested modification often indicates a **network device** is not longer operational, reflecting the reported (or deduced) effects of faults.

Construct Operation Control:

A control flow that controls the operation of **analysis constructs**, **filtering constructs**, **analysis construct sets**, **event profile sets**, and network partitions. Construct operation control is a decomposition of **surveillance control**. Construct operation control decomposes into construct control, construct set control, and **network partition control**.

Correlation Assertion:

The result of a correlation action--a correlation assertion establishes a meaningful relationship between a set of correlated items, including **alarm notifications**, **change-in state notifications**, and previous correlations.

Correlation Rule:

An **analysis rule** that is used to infer a **correlation assertion**.

Device Connectivity:

A description of the logical and physical connections existing between **network resources**.

Device Containment:

A description of the logical and physical containment relationships between **network resources**.

Disposition Rule:

An **analysis rule** that determines whether an **alarm notification** and/or one or more asserted correlations should be reported as a **reported alarm**, cleared as a **cleared alarm**, reported as an **"alarm disposition unknown" message**, held for further correlation as a **"held" alarm**, or whether a **follow-up manager inquiry** should be issued. See activity A224 Determine Alarm Disposition.

Event Notification:

A **notification** emitted by an agent describing an event. An event notification may be either an **unsolicited event notification**--sent by an **agent** system on its own initiative--or a **solicited event notification**--a notification sent by an agent in response to a request by a manager system. An **unsolicited event notification** may be an **alarm notification** or a **change-in-state event notification**. A **solicited event notification** may be a **response to a follow-up manager inquiry** or a **poll response**.

Event Profile:

A description of an **event notification** characteristics that can be used to filter incoming event notifications. Event profiles are also called event forwarding discriminators or discrimination criteria.

Event Profile Set:

A collection of **event profiles** that are used together. A particular event profile set may be activated when the **network** goes into a particular operating mode. An event profile set may also be applied to a particular **network partition**.

Event Profile Update:

A command to enable or disable the operation of a particular **event profile**. Such a command may be activated by a **disposition rule** inference in order to filter out **event notifications** that have already undergone analysis by the **alarm surveillance** system but that continue to be issued by **agents**. The purpose of this action is to reduce unnecessary traffic on the **network**.

Filtering Construct:

A data structure that is used to perform filtering. Filtering constructs may be either **event profiles** or **event profile sets**.

Filtering Construct Control:

A control flow that controls the operation of **filtering constructs** and **event profile sets**. Filtering construct control is a decomposition of **construct operation control**. Filtering construct control is specialized to individual event profile control and **event profile set control**.

Event Profile Set Control:
A control flow that controls the operation of filtering constructs sets. Event Profile set control is a decomposition of **filtering construct control.**

Follow-up Manager Inquiry:
A request for information about specific variable values made to a **network device**, such as a (**SNMP** or **CMIP**) GET operation to retrieve **MIB** variables.

GET-type poll:
A poll **message** that checks if the device is operational and retrieves information from the device. Information is retrieved (in **CMIP** or **SNMP**) using GET operations against **MIB** variables.

GET-type poll Response:
A response to a **GET-type poll.**

Health Index Computation Function:
A control flow that represents the algorithm by which the **health index value** is calculated.

Health Index Value:
The numeric result of a health index computation. Health index value is a subtype of **summary report.**

"Held" alarm notification:
An **alarm notification** that is being held for further correlation. **Disposition rules** are used to infer that particular alarm notifications should be held.

Log Inquiry:
A request for information from a log. The information usually consists of logged **event notifications** that will be used for correlation purposes.

Log Responses:
A response to a **log inquiry.**

Log Transaction Request:
A **log update** or **log inquiry.**

Log Update:
A request to update an event log; i.e, to add a new log record describing the receipt of an **event notification** or some action taken on an **alarm notification.**

Manager Inquiry:

A **message** sent by an **manager** system to an **agent** requesting information about the status of a **resource**. A manager inquiry may be a **poll** or a **follow-up manager inquiry**.

Manual Request to Poll:

A request issued by an network administrator at a terminal to initiate a polling action.

Match Results:

The result of matching incoming **poll responses** to a list of resources being polled--indicating non-responding resource agents.

Message:

An high-level, incoming or outgoing transmission that is encoded in a **network management protocol** (**SNMP** or **CMIP**).

Polling Message Structure Conventions:

A set of conventions for structuring polling **messages**.

Meta-Construct Control Command:

A generalized IDEF control that represents both **mode change commands** and **schedule construct control**.

Mode Change Command:

A control flow that changes the operation of the **alarm surveillance** system in response to a change in operating mode. The mode change command may be issued by a human operator (or network administrator) or perhaps by an automated system. The mode change command triggers changes in the operation of **analysis construct sets**, **event profile sets**, network partitions, and **schedule constructs**. See description of Control Mode Changes activity.

Network Configuration:

For purposes of **alarm surveillance**, at present the network configuration consists of information about **network device** identity-device addresses--and information describing connectivity and containment relationships among devices. Compare with the definition of network configuration in the A Context Analysis of the Network Management Domain [DABR93]. See **Network Resource Identification Data List** and **device connectivity** and **device containment**.

Network Partition Construct Relationship:

The data flow that corresponds to the network partition relationship: a network partition together with information about its **analysis constructs**, **filtering constructs**, and schedules.

Network Partition Control:

A control flow that controls the operation of network partitions. Partition control is a decomposition of **construct operation control.**

Network Resource Identification Data List:

A list of network addresses for a set of **network resources**, together with other relevant identification information. This list may be associated with a network partition.

Network Resource Polling List:

A list of **network** addresses and other information about **network resources** that is necessary to form polling **messages**. The information in the polling list is a subset of the information in **network resource identification data list.**

Network Status Reports:

An outgoing report describing the status of a **network resource** or an entire **communications network** that is produced by an **alarm surveillance** system on the basis of analysis activity conducted by that system. Network status reports consist of **reported alarms, cleared alarms, alarm disposition unknown messages**, and **summary reports.** They are encoded as **messages** for transmission in a specific **network management protocol.**

PING-type poll:

A poll **message** that checks if a **network device** is currently operational; i.e., it "pings" the device.

Poll:

A **message** sent to an agent for a **network device** to determine if the device is operating. Two types of polls exist: **PING-type polls** and **GET-type polls.**

Poll Response:

A response to a **poll** sent by an **agent**: either a PING-Type Poll Response or a **GET-Type Poll Response.**

Poll Response Statistics:

Accumulated statistics for a set of **network devices** that, at present, are assumed to consist of: (1) **poll responses** and (2) non-responses or failures to respond. These statistics may be used to calculate the **polling time interval.**

Polled Alarm Notification:

An **alarm notification** sent by an **agent** system in response to a **PING-Type poll.**

Polling Analysis Rule:

A specialization of **analysis rule** that interprets **match results** to determine whether or not an **alarm notification** should be issued.

Polling Control:

A control flow that controls the operation of polling: the activity Poll Agents. Polling control is a decomposition of **Surveillance Control**. Polling control consists of the **Polling Time Interval Adjustment Algorithm** that controls the calculation of the **polling time interval, manual requests to poll** (to initiate polling), and message structure rules.

Polling Time Interval (PTI):

The time increment that is to elapse before the next set of **polls** is issued. The PTI is used as a control flow for several activities.

Polling Time Interval Adjustment Algorithm:

An algorithm used to calculate the **polling time interval**. The algorithm is an IDEF control to the activity Calculate Polling Time Interval.

Reported Alarm:

An **alarm notification** that has been determined to have a significant impact on the operation of the network and should be reported to the **network** administrator and/or to other destinations specified by **alarm to destination mappings**.

Request to Clear Correlations:

A control that represents a request issued by a **network** administrator or other external source to remove one or more previously asserted correlations being held by the alarm surveillance system.

Rules for Query Language Syntax and Semantics:

A control flow which represents information needed to form queries in a specific query language that is used to retrieve information from a log.

Schedule Construct:

A data structure that describes the schedule of operation for an **analysis construct, filtering construct**, or network partition.

Schedule Construct Control:

A control flow that controls the operation of **schedule constructs**. The operation of individual schedule constructs may be enabled or disabled by changes in operating mode or by a **network** administrator.

SET MIB variable:

A command that changes the value of specific **MIB** variables on a **network device**. The variables contain the addresses of **manager** systems to which the device's **agent** system sends **event notifications**. The variable "setting" action is used to define the **scope** of responsibility for an **alarm surveillance** system. It is used only by the parameterized activity Control Network Device Configuration.

Solicited Event Notification:

An **event notification** that was requested by a **manager** system. At present solicited event notifications consist of **poll responses** and **responses to follow-up manager inquiries.**

Statistical Reporting Criteria:

A control flow that describes what statistical information is computed to produce **statistical summary reports.** See statistical summary report.

Statistical Summary Report:

A type of **summary report** issued by an **alarm surveillance** system that indicates the number of **event notifications** of a specific type or types that have been emitted by a specified set of **agent** systems. Statistical summary reports can be used to show trends occurring on the **network** over a successive set of time periods. The content and format of the report is application dependent.

Summary Report:

A report issued by an **alarm surveillance** system that describes the status of a managed **communications network.** The summary report is based on an analysis of **event notifications** generated over a time period by **network resources** belonging to the **network.** This data flow consists of two more specific data flows: **statistical summary report** and **health index value.**

Surveillance Construct:

A generalized construct used to perform surveillance functions--specializable into **filtering construct** and **analysis construct.**

Surveillance Control:

A generalized, top-level, control flow that controls the operation of the **alarm surveillance** system. Surveillance control consists of **construct operation control** and **polling control.**

Suspend/Resume:

A control command issued either externally or by an internal construct control activity that suspends or resumes the operation of filtering activity or analysis activity. Suspend/Resume is a subtype of **construct operation control.**

Time Interval for Holding Correlations:

A control flow that represents the period of time for which a previously asserted correlation can be used to assert new correlations. When this time interval expires, the previously asserted correlation is removed, or cleared, so that it can no longer be used to assert new correlations.

Unsolicited Event Notification:

An **event notification** sent by an agent on its own initiative, such as **message** describing a possible **fault** that has occurred on the device. Unsolicited event notifications consist of **alarm notifications** and **change-in-state notifications.**

APPENDIX B: FUNCTIONAL AND INFORMATION MODEL CORRESPONDENCE

In this Appendix, section B.1 links data flows and control flows to particular information structures. Section B.2 describes individual entities and relationships that are created, read, updated, or deleted by particular functions in the Functional Model. Section B.3 provides types hierarchies that are important in the domain model, including data flow type hierarchies and control flow type hierarchies.

B.1 Data/Control Flow to Information Model Correspondence

This table describes the correspondence between (1) the data and control flows in the Functional Model, described in section 5 of this report and (2) the entities and relationships in the Information Model, described in section 6. Only correspondences for data flows, control flows, entities, and relationships at the most specific levels of generality are shown. Those at higher levels are not shown but are described in the definitions in Appendix A.2. Complete type hierarchies for data flows and control flows are reproduced in Appendix B.3. Certain control flows do not have corresponding entities or relationships: these are indicated accordingly. Relationships are followed by a list of all model constructs which take part in that relationship (enclosed in parentheses). Asterisks ('*') indicate model constructs which contribute only identifying information needed to describe the relationship.

Data or Control Flow	Information Model Construct	Type	Section
Agent/Alarm Relationship	Agent Transmission Relationship (*agent, event notification, *manager)	Rel'ship	6.3.2.1
Alarm Disposition Unknown Message	Alarm Disposition Report Transmission (*manager, alarm notification entity, *agent)	Rel'ship	6.3.2.2 (b)
Alarm Threshold Set Request	Change-in-Attribute Value Notification Entity	Entity	6.3.2.1 (b.2.1.3)
Alarm Threshold Update	Resource Update (*manager, change-in-operability state notification entity, change-in-attribute notification entity, *agent)	Rel'ship	6.3.2.2 (c)

Data or Control Flow	Information Model Construct	Type	Section
Alarm Notification Description	Alarm Notification Entity	Entity	6.3.1.2(b.2 .2)
Alarm-to-Destination Mapping	Alarm Disposition Report Transmission (*manager, alarm notification entity, *agent)	Rel'ship	6.3.2.2 (b)
Alarm Notification	Agent Transmission Relationship (*agent, event notification, *manager)	Rel'ship	6.3.1.2 (b.2.2)
Analysis Construct Control	Change-in-Operability State Notification Entity	Entity	6.3.2.1 (b.2.1.1)
Analysis Construct Sets	Analysis Construct Set (analysis rules, schedule)	Rel'ship	6.4.2.4 (b)
Analysis Construct Set Control	Change-in-Operability State Notification Entity	Entity	6.3.2.1 (b.2.1.1)
Change-in-State Notification (as external input to alarm surveillance system only)	Agent Transmission Relationship (*agent, event notification entity, *manager)	Rel'ship	6.3.1.2 (b.2.1)
Cleared Alarms	Alarm Disposition Report Transmission (*manager, alarm notification entity, *agent)	Rel'ship	6.3.2.2 (b)
Configuration Updates	Resource Update	Rel'ship	6.3.2.2 (c)
Correlation Assertion	Correlation Assertion	Entity	6.4.1.2 (a)
Correlation Rules	Correlation Rule	Rel'ship	6.4.2.3 (a)
Device Connectivity	Resource Connection (*link device, *end-system device, *intermediary device)	Rel'ship	6.5.2.3
Device Containment	Resource Containment (*link device)	Rel'ship	6.5.2.2

Data or Control Flow	Information Model Construct	Type	Section
Disposition Rules	Disposition Rule	Rel'ship	6.4.2.3 (b)
Event Profiles	Event Profile (event notification pattern, schedule, *communicating entity)	Rel'ship	6.4.2.2
Event Profile Update	Change-in-Operability State Notification Entity	Entity	6.3.2.1 (b.2.1.3)
Filtering Construct Control	Change-in-Operability State Notification Entity	Entity	6.3.2.1 (b.2.1.3)
Event Profile Sets	Event Profile Set (event profiles, schedule)	Rel'ship	6.4.2.4 (a)
Event Profile Set Control	Change-in-Operability State Notification Entity	Entity	6.3.2.1 (b.2.1.3)
Follow-up Manager Inquiry	Manager Inquiry Transmission (*manager, manager inquiry, *agent)	Rel'ship	6.3.1.2 (a.2)
GET-type Poll	Manager Inquiry Transmission (*manager, manager inquiry, *agent)	Rel'ship	6.3.1.2 (a.2)
GET-type Poll Response	Agent Transmission Relationship (*manager, *agent, get-type poll response)	Entity	6.3.1.2 (b.1.2)
Health Index Computation Function	None	N/A	
Health Index Value	Health Index Value Entity	Entity	6.4.1.2 (d)
"Held" Alarm Notification	Alarm notification entity	Entity	6.3.1.2 (b.2.2)
Log Inquiries	Log Inquiry Construct Pattern	Entity	6.4.1.1

Data or Control Flow	Information Model Construct	Type	Section
Log Responses	All Specializations of Transmission Relationships (*agent, event notification, *manager, manager inquiry)	Rel'ship	6.3.2.1 and 6.3.2.2
Log Updates	" " " "	" "	" "
Manual Request to Poll	None	N/A	
Match Results	Poll Response Record (manager inquiry, solicited event notification)	Rel'ship	6.4.2.6 (a)
Mode Change Command	None	N/A	
Network Partition Construct Relationship	Network Partition (network resources, schedule, analysis construct sets, event profile sets, agent responsibility)	Rel'ship	6.4.2.5
Network Partition Control	Change-in-Operability State Notification Entity	Entity	6.3.2.1 (b.2.1.3)
Network Resource Identification Data List	Network Partition (agent responsibility)	Rel'ship	6.4.2.5
Network Resource Polling List	Network Partition (agent responsibility)	Rel'ship	6.4.2.5
PING-type Polls	Manager Inquiry Transmission (*manager, manager inquiry, *agent)	Rel'ship	6.3.1.2
PING-type Poll Response	Manager Inquiry Transmission (*manager, manager inquiry, *agent)	Rel'ship	6.3.1.2 (b.1.1)
Poll Response Statistics	Response Statistic Structure (network resource, polling time interval)	Rel'ship	6.4.2.6

Data or Control Flow	Information Model Construct	Type	Section
Polled Alarm Notification	Agent Transmission Relationship (*manager, *agent, alarm notification entity)	Rel'ship	6.3.1.2 (b.2.2)
Polling Analysis Rules	Polling Analysis Rule	Rel'ship	6.4.2.3 (c)
Polling Message Structure Conventions	None	N/A	
Polling Time Interval	Polling Time Interval Entity	Entity	6.4.1.2 (c)
Polling Time Interval Adjustment Algorithm	None	N/A	
Reported Alarms	Alarm Disposition Report Transmission (*manager, alarm notification entity, *agent)	Rel'ship	6.3.2.2 (b)
Response to Follow-up Manager Inquiry	Agent Transmission Relationship (*agent, manager inquiry response, *manager)	Rel'ship	6.3.1.2 (b.1.2)
Schedule Construct	Schedule	Entity	6.4.1.2
Schedule Construct Control	Change-in-Operability State Notification Entity	Entity	6.3.2.1 (b.2.1.3)
SET MIB Variable Commands	Resource Update	Rel'ship	6.3.2.2 (b)
Suspend/Resume	Change-in-Operability State Notification Entity	Entity	6.3.2.1 (b.2.1.3)

B.2 Modified CRUD Table

This table provides information on what IDEF0 activities perform create, read, update, and delete actions on entities and relationships in the Information Model. The IDEF0 activities in this table are lowest-level activities in the decomposition, with the exception of Activities A1 **Process Incoming Transmission** and A4 **Process Outgoing Messages**. Data flows, control

flows, entities, and relationships at higher levels of generality are marked with asterisks. Type hierarchies are provided in Appendix B.3.

Information Structure	Create	Read	Update	Delete
Agent Transmission Relationship		A215		
Alarm Disposition Report Transmission	A234	A235, A4		
Alarm notification entity	A232, A2312	A1, A215, A232, A2331, A2333		A232, A2333
Analysis Construct Set		A213b	A213b	A213b
Change-in-Attribute Value Notification Entity	A215, A22	A215, A4		
Change-in-Operability State Notification Entity	A211a, A211b, A234	A1, A232, A2331		A232
Log Inquiry Construct Pattern	A2331	A2332		
Correlation Assertion	A2331	A2333, A234	A2333	A2333
Correlation Rule		A213a, A213b, A2331	A213a, A213b	A213a, A213b
Disposition Rule		A213a, A213b, A234	A213a, A213b	A213a, A213b
Event Profile		A212a, A232 A212b	A212a, A212b	A212a, A212b
Event Profile Set		A212b	A212b	A212b
GET-type Manager Inquiry	A234 A33a, A33b	A4		
Health Index Value Entity	A24b	A4		
Manager Inquiry Response		A1, A234, A24b, A2311		

Information Structure	Create	Read	Update	Delete
Network Partition		A211a, A211b, A214a, A214b, A2313b, A32a, A32b, A32c, A33a, A33b	A214a, A214b, A32a, A32b, A32c	A214a, A214b
Network Resource		A214a, A214b, A22, A2311, A2331, A2332, A2333, A32a, A32b, A33a, A33b	A214a, A214b,	A214a, A214b
PING-Type Poll	A33b	A33c, A4		
Poll Response (PING-type)		A1, A2311		
Poll Response Record	A2311	A2312, A2313a, A2313b	A2311	A2312, A2313a, A2313b
Polling Analysis Rule		A213a, A213b, A2312	A213a, A213b	A213a, A213b
Polling Time Interval Entity	A31	A2311, A2313a, A2313b, A33a, A33b	A33a, A33b, A2311, A2313a, A2313b	
Response Statistic Structure	A2313a, A2313b	A31		
Resource Connection		A2331	A234	
Resource Containment		A2331	A234	
Schedule		A211b	A211b	A211b
Transmission Relationship	A4	A235		

B.3 Type Hierarchies

This section reproduces type hierarchies for the functional decomposition, data flows, and control flows respectively.

B.3.1 Data Flow Type Hierarchy

Major categories of inputs and outputs and their specializations are shown below.

IO1 Event Notifications
- IO11 Solicited Event Notifications
  - IO111 Responses to Follow-Up Manager Inquiries
  - IO112 Poll Responses
    - IO1111 PING-type Poll Responses
    - IO1112 Polled Alarm Notifications
    - IO1113 GET-type Poll Responses
- IO12 Unsolicited Event Notifications
  - IO121 Alarm Notifications
  - IO122 Change-in-State Notifications

IO2 Network Configuration Information
- I21 Network Configuration
  - I211 Network Resource Identification Data list
  - I212 Device Connectivity
  - I213 Device Containment
- I22 Configuration Updates

I3 Surveillance Constructs
- I31 Analysis Constructs
  - I311 Analysis Rules
    - I3111 Correlation Rules
    - I3112 Polling Analysis Rules
    - I3113 Disposition Rules
  - I312 Analysis Construct Sets
- I32 Filtering Constructs
  - I321 Event Profiles
  - I322 Event Profile Sets
- I33 Network Partition Construct Relationship
- I34 Schedule Constructs
- I35 Alarm Threshold Control Data
  - A351 Alarm Threshold SET Request
  - A352 Alarm Threshold Update

O4 Log Transaction Request
- O41 Log Updates
- O42 Log Inquiries

O5 Messages (outgoing)
- O51 Network Status Reports
  - O511 Reported Alarms
  - O512 Cleared Alarms
  - O513 Alarm Disposition Unknown Message

O514 Summary Report
O5141 Health Index Value
O5142 Statistical Summary Report
O52 Manager Inquiries
O531 Polls
O5311 PING-Type Poll
O5312 GET-Type Poll
O532 Follow-Up Manager Inquiries
O53 Set MIB Variable Commands

B.3.2 Control Flow Type Hierarchy

The major categories of data control and their specializations are shown below. Specializations are shown as indentations of generalizations.

C1 Surveillance Control
C11 Polling Control
C111 Polling Interval Adjustment Algorithm
C112 Polling Time Interval
C113 Polling Message Structure Conventions
C114 Manual Request to Poll
C12 Construct Operation Control
C121 Filtering Construct Control
C1211 Event Profile Control
C1212 Event Profile Set Construct Control
C122 Analysis Construct Control
C1221 Analysis Rule Control
C1222 Analysis Construct Set Control
C123 Network Partition Control
C124 Meta-Construct Control Command
C1241 Mode Change Command
C1242 Scheduling Construct Control
C13 Suspend/Resume
C14 Summary Report Computation Criteria
C141 Statistical Reporting Criteria
C142 Health Index Computation Function
C15 Alarm Notification Control Data
C151 Alarm Notification Description
C152 Agent/Alarm Relationship
C153 Alarm-to-Destination Mappings
C2 Message Translation Rules
C21 Binary Encoding Rules
C22 Parsing and Formatting Rules
C23 Decoding Rules
C24 SNMP Community Names
C25 SNMP Community Profiles
C26 SNMP Identification Information
C27 CMIP Identification Information
C28 Forwarding Destinations

APPENDIX C: SUPPLEMENTAL IDEF0 DECOMPOSITIONS

This section describes decompositions of activity A1, Process Incoming Transmissions, and activity A4, Process Outgoing Messages for both SNMP and CMIP.

C.1 Decomposition of Process Incoming SNMP Transmissions

This section describes the specialization of Process Incoming Events as activity A1a **Process Incoming SNMP Transmissions**. The activity Process Incoming SNMP Transmissions consists of the following:

- o Check for Valid SNMP Protocol Data Units
- o Authenticate SNMP Message
- o Determine Authorization for SNMP Message
- o Decode
- o Prepare for Analysis
- o Forward

The decomposition of Process Incoming SNMP Transmissions is shown graphically in figure C.1 and described in the explanatory text below.

EXPLANATORY TEXT

A1a.1 Check for Valid SNMP Protocol Data Units

This activity examines incoming PDUs to determine they are valid SNMP PDUs.

Description: PDUs are checked to determine if they are SNMP PDUs. Valid SNMP PDUs are forwarded for decoding and conversion. Messages in other protocols are discarded.

Input: Message
Output: SNMP Message
Control: SNMP Identification Information
Parameterization: None.

A1a.2 Authenticate

This activity checks if community name in the message matches community known to the manager.

Description: If the name is known, the message is forwarded for authorization. Otherwise it is discarded.

Input: SNMP Message
Output: Authenticated SNMP Message
Control: List of SNMP Community Names known to the alarm surveillance system.
Parameterization: None

A1a.3 Determine Authorization

This activity determines the allowed level of access for the incoming SNMP message.

Description: The community profile is used to determine the allowed level of access for the incoming message. If the community profile is inconsistent with the information in the incoming message, an error is signalled.

Input: Authenticated SNMP Message
Output: Authorized SNMP Message
Control: List of SNMP Community Profiles known to the alarm surveillance system.
Parameterization: None

A1a.4 Decode

This activity decodes the SNMP PDUs in encoded form and converts the data into a native machine representation.

Description: Decoding routines based on the Basic Encoding Rules (BER) are applied to a protocol data unit (PDUs) to decode a sequence of encoded ASN.1 type tag-length-value fields. The encoded information is converted into a native machine representation that can be read by the alarm surveillance application. During the decoding process, the syntax of the PDU is checked for correctness. PDUs with syntax errors are discarded. Protocol-specific information that will not be relevant for analysis is separated and discarded. Information from separate PDUs is assembled into a single message.

Input: Authorized SNMP Message.
Output: User data for SNMP Message in native machine-readable form.
Control: The activity is controlled by decoding rules for SNMP PDUs consisting of ASN.1 encoded types
Parameterization: None.

A1a.5 Prepare for Analysis

Description: Depending on type of message, parses user data to identify and delimit all fields that will be examined in subsequent filtering and analysis activity. Formats parsed fields for subsequent filtering and analysis activity as needed.

Input: User data for SNMP Message in native machine-readable form.
Output: Formatted User Data for SNMP Message in native machine-readable form.
Control: Parsing and Formatting Rules
Parameterization: None.

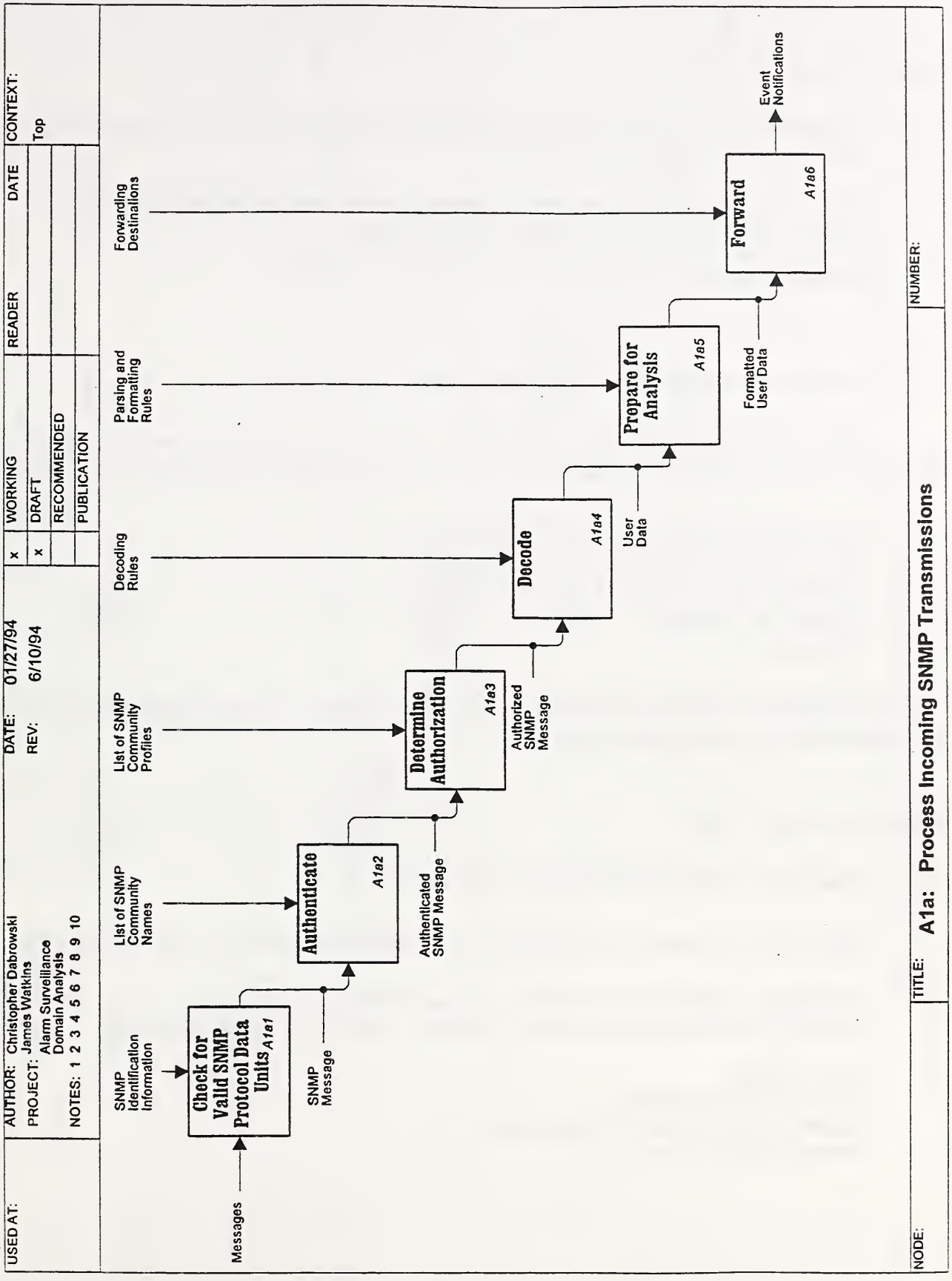


Figure C.1: Decomposition of Process Incoming SNMP Transmissions

A1a.6 **Forward**

Description: The activity forwards formatted event notifications to Activity A2, **Analyze Events** and also sends event notifications to the system log.

Input: Formatted User Data for SNMP Message in native machine-readable form.
Output: Formatted Event Notifications and Log Updates.
Control: Forwarding destinations for different types of messages.
Parameterization: None.

C.2 Decomposition of Process Incoming CMIP Transmissions

This section describes the specialization of Process Incoming Events as activity A1b **Process Incoming CMIP Transmissions.** The decomposition of this activity consists of:

- o Check for Valid CMIP Protocol Data Unit
- o Send Confirmed Mode Acknowledgement
- o Convert CMIP Protocol Data Unit (PDU)
- o Prepare for Analysis
- o Forward

The decomposition of Process Incoming CMIP Transmissions is shown graphically in figure C.2 and described in the explanatory text below.

EXPLANATORY TEXT

A1b.1 **Check for Valid CMIP Protocol Data Unit**

This activity examines incoming PDU to determine that it is a valid CMIP PDU.

Description: CMIP PDUs are checked to determine if they are CMIP messages. Valid CMIP PDUs are forwarded for decoding and conversion. Messages in other protocols are discarded.

Input: Message
Output: CMIP Transmission
Control: CMIP Identification Information
Parameterization: None.

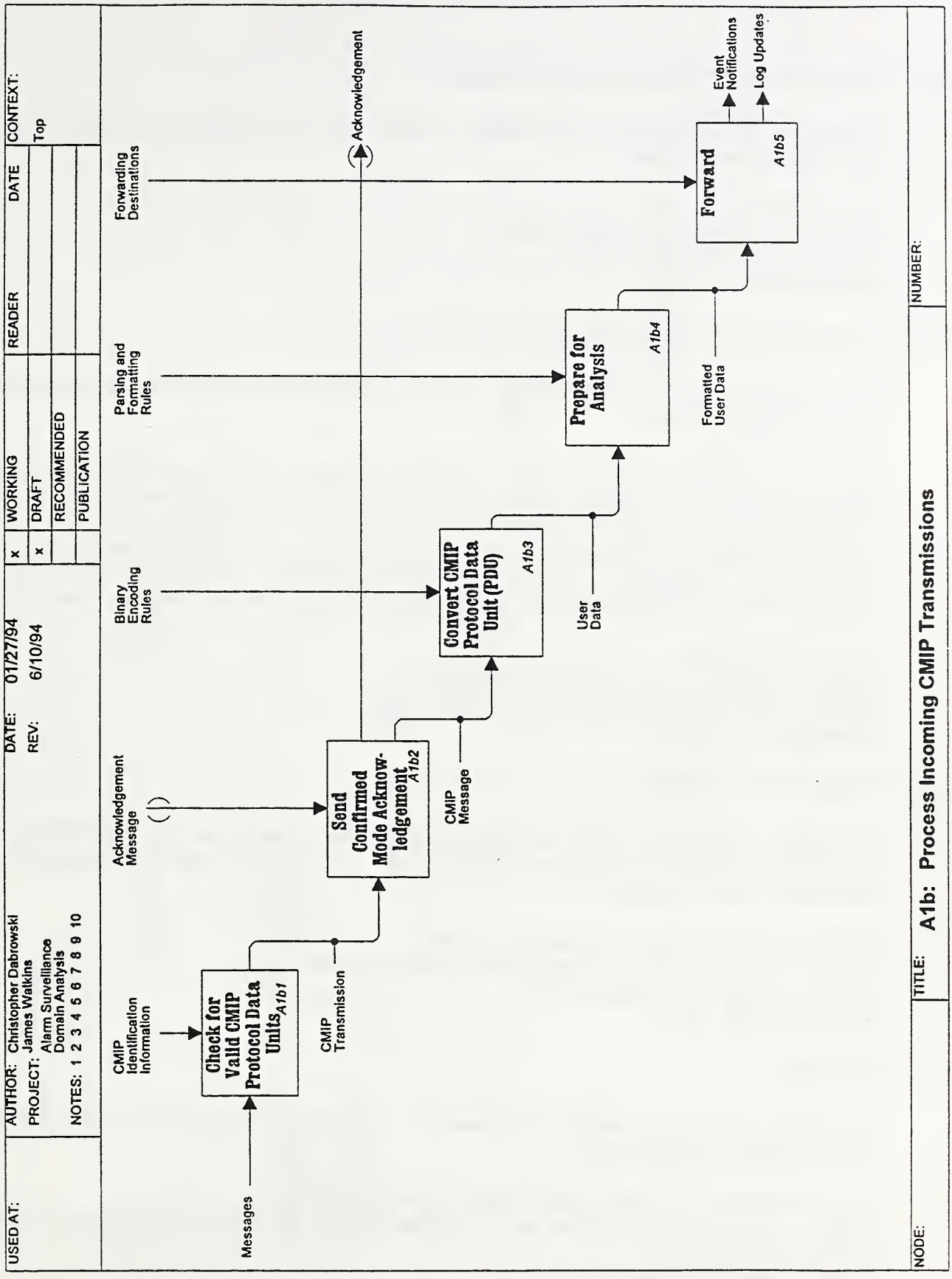


Figure C.2 Decomposition of Process Incoming CMIP Transmissions

A1b.2 Send Confirmed Mode Acknowledgement

Description: This activity checks if the message being received is confirmed mode and, if so, it sends the appropriate acknowledgement.

Input: CMIP Transmission
Output: Acknowledgement, CMIP Message
Control: Acknowledgement Message
Parameterization: None

A1b.3 Convert CMIP Protocol Data Unit (PDU)

This activity decodes a CMIP PDU in encoded form and converts the data into a native machine representation.

Description: The event notification is first examined to determine what encoding rules were used to encode the notification. Appropriate decoding routines are then applied to a protocol data unit (PDU) to decode a sequence of encoded ASN.1 type tag-length-value fields. The encoded information is converted into a native machine representation that can be read by the alarm surveillance application. During the decoding process, the syntax of the PDU is checked for correctness. PDUs with syntax errors are discarded. Protocol-specific information that will not be relevant for analysis is separated and discarded.

Input: CMIP message
Output: User Data in native machine-readable form.
Control: Binary Encoding Rules to decode CMIP PDUs
Parameterization: None.

A1b.4 Prepare for Analysis

Description: Depending on type of message, parses user data to identify and delimit all fields that will be examined in subsequent filtering and analysis activity. Formats parsed fields for subsequent filtering and analysis activity as needed.

Input: User Data in native machine-readable form.
Output: Formatted User Data in native machine-readable form.
Control: Parsing and Formatting rules.
Parameterization: None.

A1b.5 Forward

Description: Sends event notifications to event log. Depending on type of event, sends to different activities within **Analyze Events**.

Input: Formatted User Data in native machine-readable form.
Output: Formatted Event Notifications, Log Inquiry Results, and Network Configuration (routed to appropriate destinations)
Control: Forwarding Destinations.
Parameterization: None.

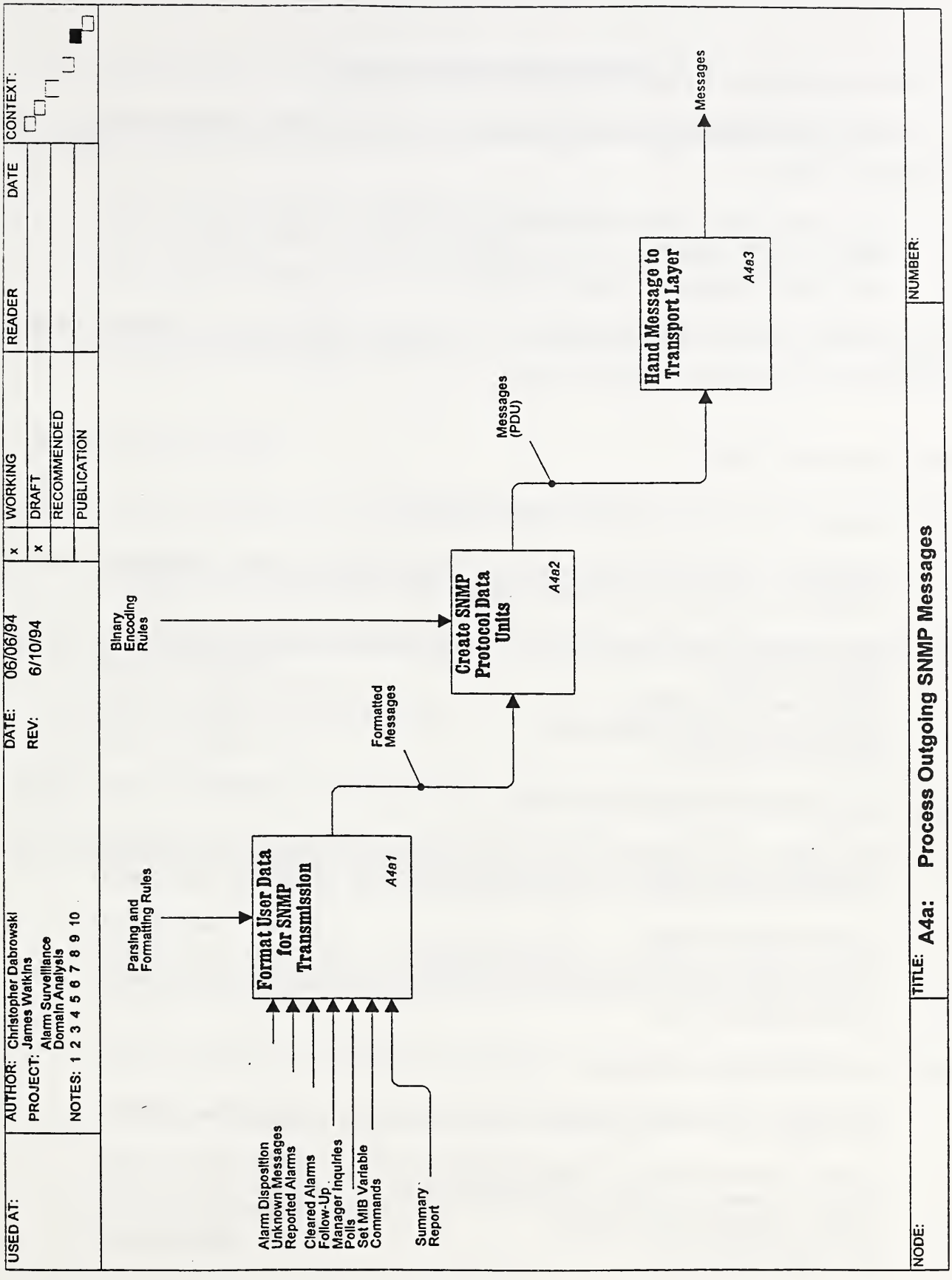


Figure C.3: Decomposition of Process Outgoing SNMP Messages

C.3 Decomposition of Process Outgoing SNMP Messages

This section describes the decomposition of **Process Outgoing SNMP Messages**, shown in figure C.3, into:

- o A4a1 Format User Data for SNMP Transmission
- o A4a2 Create SNMP Protocol Data Units
- o A4a3 Hand Message to Transport Layer

These activities result in the conversion of a message from internal format to a format appropriate for the Internet Transport Layer.

EXPLANATORY TEXT:

A4a1 Format User Data for SNMP Transmission

Description: The activity formats user data portion of outgoing message as necessary for subsequent encoding and transmission as an SNMP message.

Input: Reported Alarms, Cleared Alarms, "Alarm Disposition Unknown" messages, Follow-Up Manager Inquiries, and Polls.
Output: Formatted Messages.
Control: Parsing and Formatting rules.
Parameterization: None.

A4a2 Create SNMP Protocol Data Units

Description: Protocol-specific information is added to the message to form the structure of SNMP Protocol Data Units (PDUs). The protocol data unit is then encoded into binary format.

Input: Formatted Messages.
Output: Formatted Messages in binary PDU format.
Control: The activity is controlled by Binary Encoding Rules (BER) for SNMP PDUs.
Parameterization: None.

A4a3 Hand Message to Transport Layer

Description: The message is handed to the Transport layer within the Internet protocol suite.

Input: Formatted Messages in binary PDU format.
Output: Formatted Messages in binary PDU format.
Control: (Implementation specific)
Parameterization: None.

C.4 Decomposition of Process Outgoing CMIP Messages

This section describes the decomposition of **Process Outgoing CMIP Messages**, shown in figure C.4, into:

- o A4b1 Format User Data for CMIP Transmission
- o A4b2 Create CMIP Protocol Data Units
- o A4b3 Hand Message to Presentation Layer

These activities result in the conversion of a message from internal format to a format appropriate for the OSI Presentation Layer.

EXPLANATORY TEXT:

A4b1 Format User Data for CMIP Transmission

Description: The activity formats user data portion of outgoing message as necessary for subsequent encoding and transmission as an CMIP message.

Input: Reported Alarms, Cleared Alarms, "Alarm Disposition Unknown" Messages, Follow-Up Manager Inquiries, and Polls.
Output: Formatted Messages
Control: Parsing and Formatting Rules.
Parameterization: None.

A4b2 Create CMIP Protocol Data Units

Description: Protocol-specific information is added to the message to form the structure of a CMIP Protocol Data Unit (PDU). The protocol data unit is then encoded into binary format.

Input: Formatted Messages
Output: Formatted Messages in binary PDU format.
Control: The activity is controlled by Binary Encoding Rules (BER) for CMIP PDUs.
Parameterization: None.

A4b3 Hand Message to Presentation Layer

Description: The message is handed to the Presentation layer within OSI protocol suite.

Input: Formatted Messages in binary PDU format.
Output: Formatted Messages in binary PDU format.
Control: (Implementation specific)
Parameterization: None.

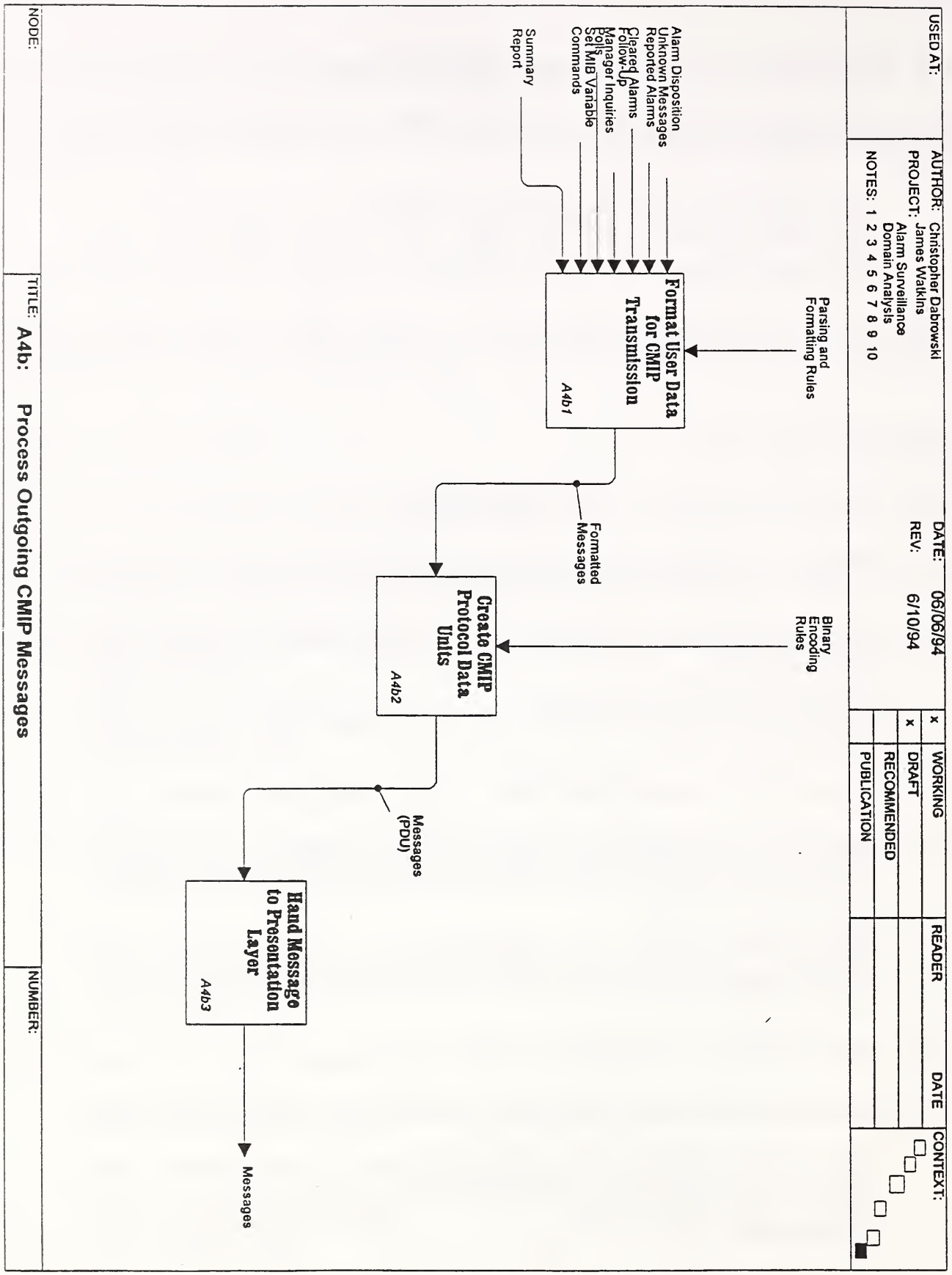


Figure C.4: Decomposition of Process Outgoing CMIP Messages