Systems Management Functions in OSI Management

Ching-Sung Lu, Cheng-Mu Shioa, Yen-Cheng Chen, Yie-Sheng Chiou, Chu-Yu Wu,
Pin-Fu Chen, Yeau-Whang Tsai, Kuang-Leng Fan, and Hey-Chyi Young

Information Technology Laboratory
Telecommunication Laboratories, MOTC
Yang-Mei, Taiwan, R.O.C.

Abstract

This paper will introduce the systems management functions in OSI management. The systems management functions together provide a generic platform of systems management capabilities for various management applications. Therefore, it is important for developing OSI management applications to realize the services provided by the systems management functions. Currently, the standards for systems management functions are at various stages of development. In this paper, we will introduce the following systems management functions with the final IS status: the Object Management Function, the State Management Function, Attributes for Representing Relationships, the Alarm Reporting Function, the Event Report Management Function, the Log Control Function, and the Security Alarm Reporting Function. For each systems management function, we will describe the provided services, generic definitions, and important concepts related to the conceptual models adopted by the systems management functions. Further, the relationships among systems management functions will be also discussed.

1. Introduction

Open Systems Interconnection (OSI) has become a pervasive model for defining how heterogeneous computer systems can communicate with each other. Thus, ISO has developed a lot of OSI standards dealing with computer communication. However, an OSI-based system or network will be of little use if it cannot be managed properly and efficiently. Therefore, there is a recognized need to address the management issues in an OSI environment. The activities that address these problems are called OSI management. In summary, OSI management is the facilities to control, coordinate and monitor the resources which allow communications to take place in the OSI environment.

OSI management standards are maturing rapidly. The ultimate goal of these standards is to enable the development of interoperable, multi-vendor products for the management of computer and communications systems and networks. In a network with interoperable, multi-vendor products, the network manager is allowed to remotely monitor and control network resources residing on network components developed by different vendors. To achieve this requirement, there must be a common method for transferring the management commands and information. Moreover, there must be a common view of management information. To foster the information exchange in a consistent way, OSI management has defined standard management services and their protocol, known as Common Management Information Services and Protocol (CMIS/P) [3-4]. In addition, a set of standards, collectively called the Structure of Management Information (SMI) [14-16], has also been developed to provide a standard representation of management information. To further define specific services and protocols to support OSI management, a set of standards, known as the System Management Functions (SMFs) [6-12], is being developed.

The SMF standards are at various stages of development, ranging from working proposals to CDs, DISs, and ISs. Additional SMFs will be developed as needs are identified. Among the SMFs, the Object Management Function [6], the State Management Function [7], Attributes for Representing Relationships [8], the Alarm Reporting Function [9], the Event Report Management Function, [10], the Log Control Function [11], and the Security Alarm Reporting Function [12], are ISs. In this paper, we will concentrate on the seven SMFs. In addition to the introduction of the above SMFs, this paper is also intended to discuss the roles of SMFs within the OSI systems management model. Further, we will present the relationships among the SMFs, CMIS, and five upper Specific Management Functional Areas (SMFAs) [2]. The rest of this paper is organized as follows. In Section 2, the OSI systems management model will be shown. Section 3 presents the functional aspects of OSI management. Section 4 introduces each SMF in more detail. Finally, a conclusion is given in Section 5.

2. OSI Systems Management Model

The OSI systems management provides mechanisms for the monitoring, control, and coordination of the resources within the OSI environment and OSI protocol standards for communicating information pertinent to those resources. The resources could be workstations, personal computers, printers, modems, circuits, processes, etc. Since the OSI systems management adopts an object-oriented approach, these managed resources are abstractly represented as objects with defined properties. These objects are called managed objects [2]. Each managed object is defined in terms of attributes which the OSI management concerns, operations that may be performed upon it, notifications that it may issues, and its relationships with other managed objects. Further, the repository of the managed objects is called the Management Information Base (MIB) [2]. Therefore, the information aspects of the OSI systems management model are essentially an object-oriented model of management information. Based upon the object-oriented principles, the concepts such as inheritance, allomorphism, containment and naming related to objects are also applied in the management information model.

In general, the OSI environment being managed is distributed. Thus, the individual components of the management activities are themselves distributed. This implies that the OSI systems management model is a distributed model [5]. That is, management applications perform the management activities in a distributed manner. Therefore, the OSI systems management is to support the distributed management of managed objects. The architecture of the OSI systems management is shown in Figure 1. Since the managed resources have been represented as managed objects, management activities are effected through the manipulation of managed objects. Therefore, as shown in Figure 1, the interactions are abstracted in terms of management operations performed upon managed objects and the notifications emitted by managed objects.

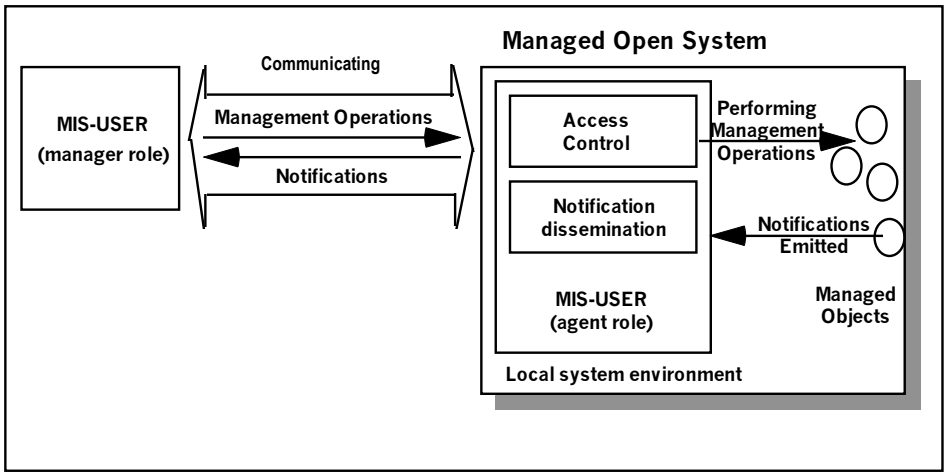

Figure 1. Architecture of OSI Systems Management.

For the purposes of systems management, management applications are categorized as MIS-Users, which are allowed to take one of two possible roles, either a manager role or an agent role. The MIS-User taking the role of an agent is responsible for the management of the managed objects within its local system environment. The MIS-User taking the role of a manager is charged with one or more management activities. The interactions between MIS-Users acting in the role of manager and agent respectively are realized through the exchange of management information. The communication is accomplished following the OSI protocols, and the communication services for the OSI systems management are supported by the CMISE. Through the communication services, the manager could issue management operations to the agent, and the agent could disseminate notifications emitted by managed objects to the manager.

3. Functional Aspects of OSI Management

To develop functions for the support of OSI systems management, ISO/IEC has partitioned systems management activities into five Specific Management Functional Areas (SMFAs) [2]: Configuration Management (CM), Fault Management (FM), Performance Management (PM), Security Management (SM), and Accounting Management (AM). This also points out the major requirements in the OSI systems management. For each requirement, one can develop individual management functions to satisfy the needs of the specific functional area. However, since there exists overlap among the requirements, the management functions applicable to one SMFA are also often applicable to other SMFAs. For example, each SMFA must have management functions to create or delete the managed objects which the SMFA concerns and to examine or modify characteristics of these managed objects. Therefore, much redundant effort will be taken if we independently develop management functions for each SMFA. For effective development of management applications, there is a need to identify these essential management functions. These basic management functions are known as the System Management Functions (SMFs).

The SMFs together provide a generic platform of systems management capabilities for various management applications. Among the SMFs, the Object Management Function [6], the State Management Function [7], Attributes for Representing Relationships [8], the Alarm Reporting Function [9], the Event Report Management Function, [10], the Log Control Function [11], and the Security Alarm Reporting Function [12], are ISs. The following SMFs are under development: Security Audit Trail Function, Objects and Attributes for Access Control, Accounting Metering Function, Workload Monitoring Function, Test Management Function, and Summarization Function [18]. Recently, the following SMFs are also to be developed: General Relationship Model Function, Management Domain Function, Management Knowledge Management Function, Response Time Monitoring Function, Scheduling Function, and Time

Management Function [17]. Hence, as needs are identified, additional SMFs can be further derived. Figure 2 shows the functional hierarchy of SMFs and SMFAs.

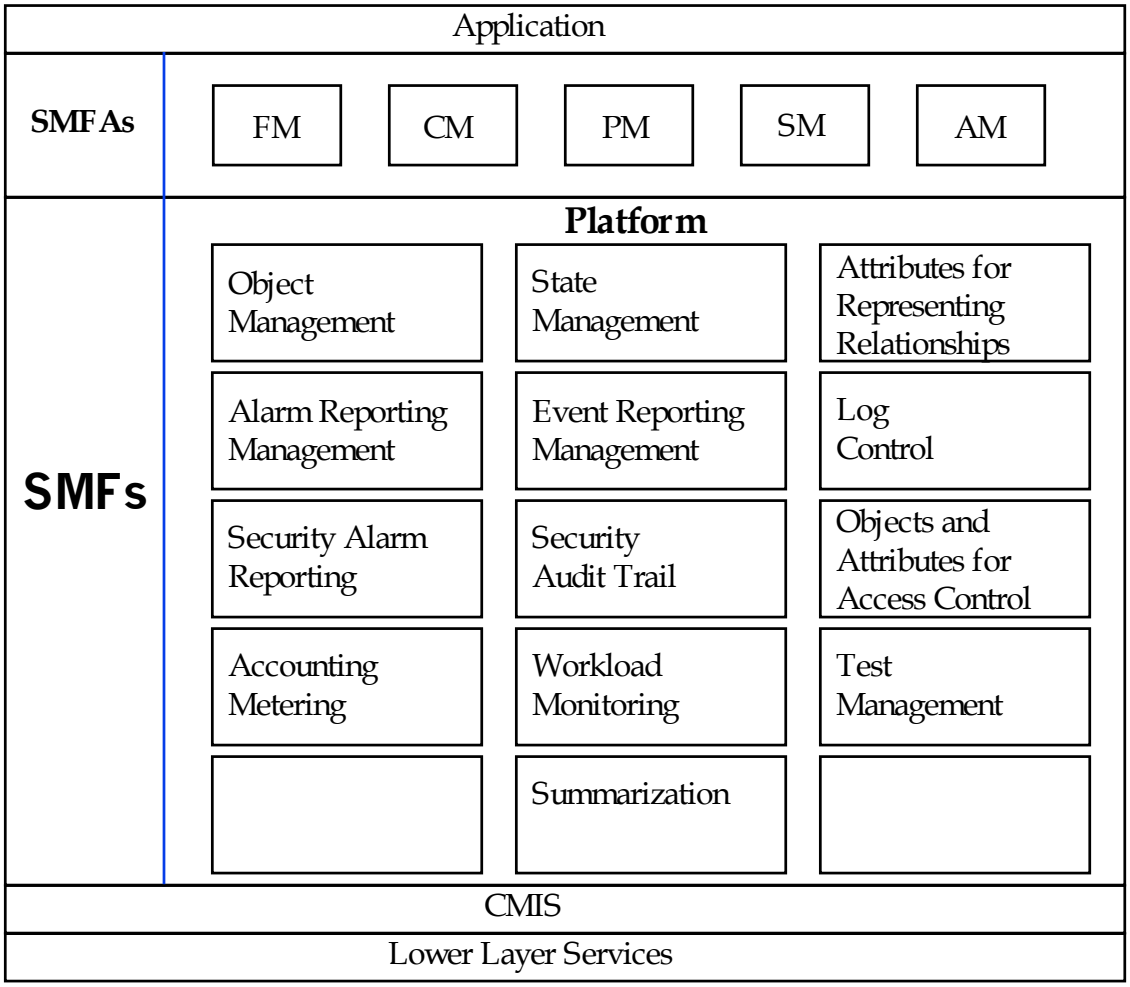

Figure 2. Functional hierarchy of SMFs and SMFAs.

4. Systems Management Functions

The standards for systems management functions define the services and, if appropriate, the functional units and generic definitions of managed objects required for each specific systems management function. In the following, we will introduce seven SMFs with the final IS status. We will introduce their generic features including the provided services, the adopted models, and related concepts of their approaches. In addition, the relationships among SMFs, CMIS, and SMFAs will be briefly discussed.

4.1. Object Management Function

It has been shown that the managed resources are abstractly represented as objects with defined properties. It implies that the monitoring of resources corresponds to reading appropriate attributes of managed objects. Besides, the control of managed resources involves management operations on managed objects. Therefore, the MIS-User needs the ability to create and delete managed objects, examine and modify the values of attributes of managed objects, and be made aware of the changes in the configuration of managed objects. The Object Management Function (OMF) [6] supports the above requirements.

Managed objects can be created, and values of attributes of managed objects can be changed in three distinct ways. One way is through configuration processes in the local system environment, which are outside the scope of OSI. The second way is through the N-layer operation and/or the layer management of an open system. The last way is through the OSI systems management services, which SMFs are interested in. These OSI object management services are described in OMF. In OMF, two kinds of services are supported. One is to support the reporting of creation and deletion of managed objects and the reporting of changes to attribute values of managed objects. The other is through pass-through services for the creation and deletion of managed objects, performing actions upon managed objects, attribute changing, attribute reading and event reporting. The pass-through services are used in order that different parts of systems management functions can define operations or notifications independently to their underlying mapping communication service. This enables the specification of SMFs to be used across a range of underlying communications services by other systems management functions or managed objects. Currently, only the mapping onto CMIS is defined in OSI standards. Through the use of pass-through services, when a systems management function defines specific systems management services, then these services will be mapped directly onto the CMIS services. The OMF defines the following pass-through services: PT-CREATE, PT-DELETE, PT-ACTION, PT-SET, PT-GET, and PT-EVENT-REPORT. The PT-CREATE service is responsible for the mapping of creating a managed object. The deletion and action performed on a managed object is through the use of the PT-DELETE and PT-ACTION service respectively. In addition, the PT-SET service is the attribute oriented service which is responsible for adding new members into a set-valued attribute, removing members from a set-valued attribute, and replacing values of an attribute with default or supplied values. In addition, reading specific attributes of a managed object can be accomplished by means of the PT-GET service. The notification emitted by a managed object is through the PT-EVENT-REPORT service.

Since management operations on managed objects are required in almost all management functional areas, the OMF provides the object management service for five upper SMFAs as well as the other SMFs. Hence, the OMF is essentially the base part of the SMFs. Within the OMF, the control of the reporting services is provided by the control mechanism of the Event Report Management Function, which will be

discussed in Section 4.5. In addition, the pass-through services have close relationships with the CMIS service because of their direct mappings.

4.2. State Management Function

The major purpose of monitoring a managed resource is to see its operability and availability such that proper controls can be further performed. The operability and availability of a managed resource is in terms of the current states that the managed resource resides on. Therefore, the MIS-User needs the ability to examine and be notified of state changes, to monitor the overall operability and usage of resources in a consistent manner, and to control the general availability of specific resources. To achieve the above requirement, the State Management Function (STMF) [7] provides for the examination, setting and notification of changes in the management state of existing managed objects. Further, to provide a standardized OSI management technique for dealing with management states, the STMF defines the general state attributes and operations that can be part of any managed object definition.

The management state of a managed object represents its instantaneous condition of availability and operability from the point of view of management. The three primary factors, *Operability*, *Usage*, and *Administration*, affect the management state of a managed object with regard to its corresponding resources' availability. Some managed objects may not be affected by all three of these factors. The *Operability* factor denotes whether or not the resource is physically installed and working, if applicable. The *Usage* factor indicates whether or not the resource is actively in use at a specific instant, and if so, it also indicates whether or not it has spare capacity for additional users at that instant. The *Administration* factor denotes the permission to use or prohibition against using the resources, imposed through the management services. In the STMF, the three factors are corresponding to the *Operational state*, *Usage state*, and *Administrative state*, respectively. Moreover, corresponding state attributes are defined to represent these states.

The operability of a resource is described by the *Operational state* attribute, which has two possible values: *Disabled* and *Enabled*. It is the natural operation of the resource that cause operational state transitions to occur. Therefore, management cannot request the change of the operational state of a managed object. Management can only gather information about the operational state of a managed object, i.e., the operational state is read-only in nature. The usage of a resource is described by the *Usage* state attribute, which has three possible values: *Idle*, *Active* and *Busy*. Managed objects whose associated resource supports only one user do not exhibit the *Active* usage state. In addition, for those managed objects whose resource do not limit the number of users, the *Busy* usage state is prohibited. Similar to the *Operational* state, the *Usage* state is read-only. The administration of managed objects operates independently of the operability and usage of the

managed objects and is described by the *Administrative* state attribute, which has three values: *Locked*, *Unlocked* and *Shutting Down*.

There are specific related events whose activities will cause state transitions. The specific events that will affect the state transition are also defined in the STMF. For the operational state, the STMF defines two events: *Enable* and *Disable*. The *Enable* (*Disable*) event will cause a transition to the *Enabled* (*Disabled*) operational state. For the usage state, the STMF defines four events: *New user*, *User quit*, *Capacity increase* (CI), and *Capacity decrease* (CD), which are used for reflecting the activities in using the managed resource. In addition, four specific events, *Unlock*, *Lock*, *Shut down*, and *User quit*, are defined for the administrative state.

As an event causes a state transition, the manager must have the ability to be made aware of the state change. The STMF defines the state change reporting service, which allows an MIS-User, in the agent role, to report the changes in the values of managed objects state attributes. The control of the state change reporting service is provided by the Event Report Management Function. Besides, the pass-through services defined in the OMF are used for managing the state attributes of managed objects.

4.3. Attributes for Representing Relationships

For a management environment, there is a need to examine the relationships among various parts of a management system or among management systems. This is to identify how the operation of one part of the system depends upon or is depended upon by other parts. In addition, the management user also needs the ability to change the relationships and to be notified of such relationship changes. Therefore, a relationship management function should be provided for an application process for the purpose of systems management. The Attributes for Representing Relationships (ARR) standard [8] describes this management function. In general, there exist several approaches for representing relationships. The relationship management gives a standard means of representing relationships among managed objects. That is, the standard indicates which attributes are to be included in managed objects to represent relationships.

In a relationship between two managed objects, one managed object may play a different role with respect to the other managed object. The role which a managed object plays in a relationship is called the *relationship role*. The relationship role is described using the *role attributes* of managed objects. Since managed objects interact with each other in various ways to reflect the complicated management activities, the relationships among managed objects are of various kinds essentially. According to different types of

relationships, the standard has defined several relationship roles and role attributes to support the relationship management.

As described previously, it is necessary to provide various kinds of relationships in OSI management. All relationships can be *direct* or *indirect*. A direct relationship exists between two managed objects when some portion of management information associated with one managed object expressly identifies the other managed object with which it has a relationship. An indirect relationship is a relationship deduced from the concatenation of two or more direct relationships. Figure 3 shows both direct and indirect relationships.

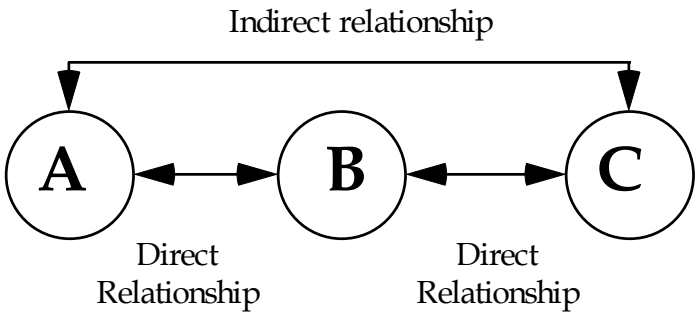

Figure 3. Direct and Indirect Relationships.

Moreover, each relationship may be either *symmetric* or *asymmetric*. The symmetric (asymmetric) relationship is the one between two managed objects when the set of generic rules governing their interactions and the roles of the two managed object are identical (different).

In addition to the above natures of relationships, managed objects may be related in one of the following three categories of relationships: *containment relationships*, *reciprocal relationships*, and *one-way relationships*. The ARR standard defines five types of reciprocal relationships: s*ervices relationships*, *peer relationships*, *fallback relationships*, *back-up relationships*, and *group relationships*. The services relationship is an asymmetric relationship denoting that the first of a pair of managed objects acts as a service provider and the second is the service user. A peer relationship is a symmetric relationship under which pairs of similar managed objects communicate. A fallback relationship is an asymmetric relationship denoting that the second of a pair of managed objects has been designated as a fallback or "next preferred choice" to the first managed object. A back-up relationship is an asymmetric relationship denoting that the second of a pair of managed objects is currently active and performing a back-up function in place of the first one. A group relationship is a relationship between two managed objects where one belongs to a group represented by the other.

In addition to describing the properties and kinds of relationships in OSI management, the relationship management also provides the controlling and monitoring of these relationships. That is, the attributes representing relationships can be read or set via management operations such as PT-GET and PT-SET services. Further, the relationship management also defines a notification type which is used to report the change in the value of one or more relationship attributes of a managed object. The relationship change reporting services could be controlled by event report management function, and may exist independently of the control mechanism in event reporting management.

4.4. Alarm Reporting Function

It is important in maintaining system operations to have the capability of detecting faults or abnormal conditions before disaster effects are felt by the system user. Therefore, a monitoring mechanism of service degradation must be provided for maintaining the service quality and preventing worse conditions. Degradation of service can be monitored by measuring various activities such as error rates, values of gauges and counters, and assessing trends. Further, when an abnormal situation is detected via the monitoring mechanism, an alarm may be reported such that some management activities are expected and the system user can realize which appropriate operations should be performed. Therefore, the Alarm Reporting Function (ARF) [9] supports the monitoring mechanism with the alarm reporting service.

Alarms are specific types of notifications concerning detected faults and abnormal conditions. Control of notifications can be accomplished by the use of the event report management function. Hence, the control mechanism of the alarm reporting service is provided by the event reporting function, which will be introduced in Section 4.5. By defining the parameters and semantics in the attributes of a specific CMIS M-EVENT-REPORT service [3], the ARF specifies its alarm reporting service. First, the ARF defines five basic categories of alarms: *communications alarm*, *quality of service alarm*, *processing error alarm*, *equipment alarm*, and *environmental alarm*. These types of alarms are identified in the event type attribute. Communication alarms are associated with the procedures and/or processes required to convey information from one point to another. Quality of service alarms concern the degradation in the quality of services. Processing error alarms are principally associated with software or processing faults, while the faults occurring in equipment will result in equipment alarms. An environment alarm concerns a condition relating to an enclosure in which the equipment resides.

For each alarm, more detailed information is carried in the event information attribute. In the following, we will introduce some significant parameters which classify various alarm reports. One

mandatory parameter is the *probable cause* parameter, which provides further qualification about the problem that generated the alarm. A set of the probable causes could be involved with a particular alarm type. The *perceived severity* parameter defines six severity levels, which provide an indication of how it is perceived that the capability of the managed object has been affected. The levels which represent service affecting conditions ordered from most severe to least severe are *Critical*, *Major*, *Minor* and *Warning*. In addition to the four severity levels, this parameter also defines two levels: *Cleared* and *Indeterminate*. The *Cleared* level indicates the clearing of one or more previously reported alarms. And, the *Indeterminate* level indicates that severity level cannot be determined. The *trend indication* parameter specifies the current trend of the managed object. There are three possible values: *More Severe*, *No Change*, and *Less Severe.* Besides, the adopted method of detecting trends and providing a warning is through the use of thresholds on counters and gauges. When a threshold is crossed, an alarm is reported and the related information is carried in the *threshold information* parameter.

4.5. Event Report Management Function

When significant changes happen in the activities of managed resources, there must be an efficient methodology to let the manager be aware of these changes as soon as possible. A potential solution to meet this requirement is the management by exception. From the viewpoint of an object-oriented approach, the notifications emitted by managed objects can offer this capability. However, in the OSI management, it is not necessary that each notification must be sent to the manager, since some notifications may be not actually useful or meaningful for systems management. Therefore, there is a need to provide a control mechanism to filter out useless notifications and to forward the significant ones to proper destinations. The Event Report Management Function (ERMF) [10] supports the above requirements.

The ERMF provides the management user with the following capabilities: the definition of a flexible event report control service, the specification of destinations to which event reports are to be sent, the specification of a mechanism to control forwarding of event reports, the ability for an external managing system to modify the conditions for reporting events, and the ability to designate a backup location to which event reports can be sent if the primary location is not available. The event report management model is depicted in Figure 4. The conceptual event pre-processing function receives local notifications generated from managed objects and forms the potential event reports with specific formats. The potential event reports are then distributed to all Event Forwarding Discriminators (EFDs). Each EFD is a management support object which is used to determine which event reports are to be forwarded to a particular destination during specified time periods. Each EFD contains a discriminator construct which specifies the condition that a potential event report must satisfy to be forwarded. That is, when each EFD

receives potential event reports, it will evaluate whether the condition is satisfied, and if the condition is satisfied, an event report is then forwarded to proper destinations. The event reporting management allows an open system to establish and control the discrimination and the forwarding of event reports to other open systems. The discrimination is specified through the use of discriminators. Since discriminators are managed objects, discriminators can be created, deleted, read and modified. In addition, the activity of discriminators can be suspended and resumed by means of manipulating their administrative states. Therefore, event reporting management comprises initialization, termination, suspension, resumption, event forwarding and modification, and retrieval of event forwarding conditions.

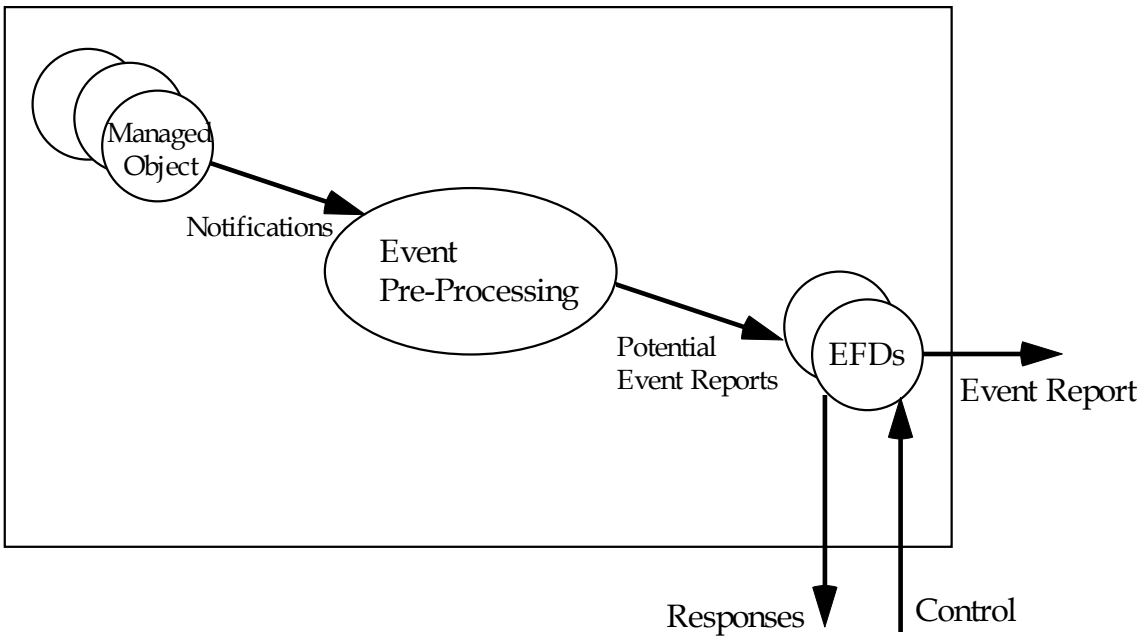

Figure 4. Event Report Management Model.

The control of the event reports is mainly via the management operations upon the EFDs. Thus, it involves object creation, deletion, and modification. These services are supported by the OMF. The services for the notifications concerning state changes are provided by the STMF. In addition, the ERMF has a close relationship with the Log Control Function, since they have similar behaviors.

4.6. Log Control Function

For the purpose of many management functions, it is necessary to be able to preserve information about events that may have occurred or operations that may have performed by or on various objects. In OSI management, the resources allocated to store such information are modeled by **logs** and **log records**

contained in the logs. That is, the log is the OSI abstraction of logging resources and acts as a repository for records. Further, the log records are managed objects that represent information stored in logs. The Log Control Function (LCF) [11] specifies a particular management function and services which allow logging of information about event reports, notifications and performed operations. The LCF provides the management user the following capabilities: the definition of a flexible log control service, the ability to modify the criteria used in logging records, the ability to determine whether the logging characteristics were modified or whether log records have been lost, the specification of the control mechanism of the time during which logging occurs, the ability to retrieve and delete log records, and the ability to create and delete logs. The model for the LCF is depicted in Figure 5.

From Figure 5, it can be seen that the logs store incoming event reports and local system notifications. In fact, logs also stores the PDUs received or transmitted by the open system. Storing such information can be accomplished via the local system notifications. Similar to the ERMF, the notifications are first transmitted to the log pre-processing function. Then, the pre-processing function generates the potential log reports with specific formats which can be sent into each log. In addition to conceptually storing the logged information, the log also can determines which information is to be logged. Hence, similar to the EFD of ERMF, each log contains a discriminator construct which specifies the characteristics a potential log record or received event report must have to be selected for logging.

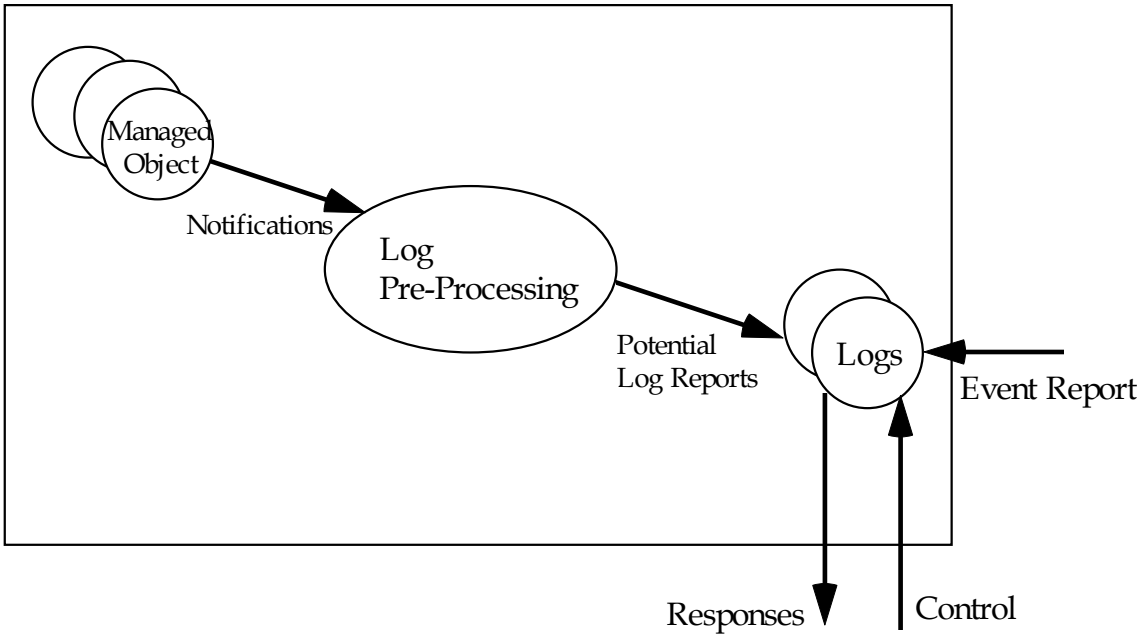

Figure 5. Log Management Model.

Besides, the logs can be controlled via management operations. In summary, the management operations can be accomplished through the use of pass-through services defined in OMF. However, it should be noted that the log records can be retrieved and deleted, but their attributes cannot be modified through the management operations. Beside the pass-through services are used for controlling logs, the notifications of state changes are via the STMF, and the reporting of log alarms is through the use of the ARF.

4.7. The Security Alarm Reporting Function

The security management user needs to be alerted whenever an event indicating an attack on system security has been detected. A security attack may be detected by a security service, a security mechanism, or another process. When a security attack is detected, a report is issued via a security alarm notification. The resulting security alarm notification may be generated by either of the communicating end users, or by any intermediate system or process between the end users. The Security Alarm Reporting Function (SARF) [12] describes the use of services and techniques to satisfy the above requirements.

Similar to the Alarm Reporting Function, the SARF defines five types of the security alarm report, which are classified in the event type attribute of M-EVENT-REPORT service. The five corresponding event types are *Integrity violation*, *Operational violation*, *Physical violation*, *Security service or mechanism violation* and *Time domain violation*. The Integrity violation indicates that information may have illegally modified, inserted or deleted. The operational violation indicates that the provision of the requested service was not possible due to the unavailability, malfunction or incorrect invocation of the service. Besides, when a physical resource has been violated in a way that suggests a security attack, the physical violation event will be reported. The security service or mechanism violation indicates that a security attack has been detected by a security service or mechanism. When some event has occurred at an unexpected or prohibited time, the time domain violation event will be issued.

For each of the above security alarms, its security alarm report will identify the cause of the security alarm, the source of the detection of the security-related event, the appropriate end users, and of the perceived severity of any misoperation, attack or breach of security, as specified by the security policy. These are specified in the parameters which together constitute the event information attribute of the security alarm notification. Among the parameter, the *security alarm severity* parameter is to specify the significance of the perceived security alarm. The parameter defines five severe levels: *indeterminate*, *critical*, *major*, *minor*, and *warning*. The classification of severe levels is similar to the one defined in the alarm reporting function.

As known, the control mechanism of the security alarm reporting service as well as the alarm reporting service is provided by the ERMF. Hence, the initiation, termination, suspension and resumption of the security alarm reporting service are provided by the initiation of event forwarding, termination of event forwarding, suspension of event forwarding and resumption of event forwarding service.

5. Conclusion

OSI management has widely received much attention in the recent years. It has been recognized to be the mainstream for the future development of network and systems management. It provides a systematic solution for the management environment with multi-vendor systems and multiple management domains. Therefore, it is quite possible that OSI management will dominate the development of network and systems management. Since the SMFs provide the generic platform for developing management applications in an OSI environment, it is important to understand the SMFs in more details. In this paper, we have introduced seven SMFs with the final IS status. We have shown why each specific SMF is required for developing management applications. Further, the generic definitions and provided services described in each SMF have also been presented. These will be helpful in understanding each SMF. Besides, we have described some related concepts adopted in the conceptual models proposed by the SMFs. These management technologies can be widely adopted in the areas of network and systems management, not limited to the scope of OSI management. There are still several features such as protocols, conformance, and detailed definitions of attributes, which are not introduced in this paper. The interested reader may consult [6-12] for more details.

References

[1] *"Information technology - Open Systems Interconnection - Basic Reference Model"* ISO/IEC IS 7498, 1984.

[2] *"Information technology - Open Systems Interconnection - Basic Reference Model - Part 4: Management Framework,"* ISO/IEC IS 7498-4, 1989.

[3] *"Information technology - Open Systems Interconnection - Management Information Service Definition - Common Management Information Service Definition,"* CCITT Rec. X.710 | ISO/IEC IS 9595, 1991.

[4] *"Information technology - Open Systems Interconnection - Management Information Protocol Specification - Common Management Information Protocol,"* CCITT Rec. X.711 | ISO/IEC IS 9596-1, 1991.

[5] *"Information technology - Open Systems Interconnection - Systems Management Overview,"* CCITT Rec. X.701 | ISO/IEC IS 10040, 1991.

[6] *"Information technology - Open Systems Interconnection - Systems Management - Part 1: Object Management Function,"* CCITT Rec. X.730 | ISO/IEC IS 10164- 1, 1991.

[7] "Information technology - Open Systems Interconnection - Systems Management - Part 2: State Management Function," CCITT Rec. X.731 | ISO/IEC IS 10164-2, 1991

[8] "Information technology - Open Systems Interconnection - Systems Management - Part 3: Attributes for Representing Relationships," CCITT Rec. X.732 | ISO/IEC IS 10164-3, 1991.

[9] "*Information technology - Open Systems Interconnection - Systems Management - Part 4: Alarm Reporting Function*," CCITT Rec. X.733|ISO/IEC IS 10164-4, 1991.

[10] "*Information technology - Open Systems Interconnection - Systems Management - Part 5: Event Report Management Function,"* CCITT Rec. X.734 | ISO/IEC IS 10164-5, 1991.

[11] *"Information technology - Open Systems Interconnection - Systems Management - Part 6: Log Control Function,"* CCITT Rec. X.735 | ISO/IEC IS 10164-6, 1991.

[12] *"Information technology - Open Systems Interconnection - Systems Management - Part 7: Security Alarm Reporting Function,"* CCITT Rec. X.736 | ISO/IEC IS 10164-7, 1991.

[13] *"Information technology - Open Systems Interconnection - Systems Management Overview,"* CCITT Rec. X.701 | ISO/IEC IS 10040, 1991.

[14] *"Information technology - Open Systems Interconnection - Management Information Services - Structure of Management Information - Part 1: Management Information Model,"* CCITT Rec. X.730 | ISO/IEC IS 10165-1, 1991.

[15] *"Information technology - Open Systems Interconnection - Structure of Management Information - Part 2: Definition of Management Information,"* CCITT Rec. X.721 | ISO/IEC IS 10165-2, 1991.

[16] "*Information technology - Open Systems Interconnection - Structure of Management Information - Part 4: Guidelines for the Definition of Managed Objects*," CCITT Rec. X.723 | ISO/IEC IS 10165-4, 1991.

[17] "*Federal Information Processing Standards: U.S. Government Network Management Profile (GNMP),"* National Institute of Standards and Technology, Version 1, July, 1992.

[18] "*Stable Implementation Agreements for Open Systems Interconnection Protocols: Part 18: Network Management*," Open Systems Environment Implementors' Workshop (OIW), September 1992.