Copyright © 1991 by the
Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street
New York, NY 10017, USA
All rights reserved as an unpublished work.

This is an unapproved and unpublished IEEE Standards Draft, subject to change. The publication, distribution, or copying of this draft, as well as all derivative works based on this draft, is expressly prohibited except as set forth below.

Permission is hereby granted for IEEE Standards Committee participants to reproduce this document for purposes of IEEE standardization activities only, and subject to the restrictions contained herein.

Permission is hereby also granted for member bodies and technical committees of ISO and IEC to reproduce this document for purposes of developing a national position, subject to the restrictions contained herein.

Permission is hereby also granted to the preceding entities to make limited copies of this document in an electronic form only for the stated activities.

The following restrictions apply to reproducing or transmitting the document in any form: 1) all copies or portions thereof must identify the document's IEEE project number and draft number, and must be accompanied by this entire notice in a prominent location; 2) no portion of this document may be redistributed in any modified or abridged form without the prior approval of the IEEE Standards Department.

Other entities seeking permission to reproduce this document, or any portion thereof, for standardization or other activities, must contact the IEEE Standards Department for the appropriate license.

Use of information contained in this unapproved draft is at your own risk.

IEEE Standards Department
Copyright and Permissions
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331, USA
+1 (908) 562-3800
+1 (908) 562-1571 [FAX]

5.3 Information System Management

Responsibility: Don Folland, Neil Croft

5.3.1 Overview and Rationale

Information System Management issues are considered in this clause. The subject is concerned with the effective management and control of the complete set of resources that comprise an information system. The tools in support of the services required by system managers need to reflect the portability and interworking attributes of open systems and fit the Open System Environment Reference Model (Figure 3-3). It is necessary to consider a variety of system management support scenarios (central management, dispersed management, or hybrid), addressing both distributed systems and standalone systems. The issues apply to application software or software components of the application platform. It is necessary to support automated management and operation of the IT infrastructure and address a wide variety of licensing scenarios. E

5.3.2 Scope

This category includes services and policies that address the administration of the overall information system required by any organization, including:

— Information Management

— Processor Management (e.g., Add new user)

— Network Management

— Configuration Management

— Security Management (e.g., Authentication, Key Management)

— Accounting Management

— Performance Management

Administration services accessible from the API may have Programming Language or Language Binding service specifications associated with them.

These services are defined to provide system and network administrator portability.

5.3.3 Reference Model

The Reference Model for system management is the same as the model shown in Figure 3-3. System management impacts all of the APIs and EEIs in the POSIX Open System Environment Reference Model. E

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

5.3.4 Service Requirements

The following services should be provided: E

5.3.4.1 Processor Configuration Management

Configuration management consists of four basic functions: identification, control, status accounting, and verification.

Identification involves specifying and identifying all components of an IT infrastructure.

Control implies the ability to agree and ''freeze'' configuration items (CIs) and then to make changes only with agreement of the appropriate named authorities. Control is concerned with ensuring that none of the CIs shown is altered or replaced and that no CIs are added without appropriate authorization.

Status accounting involves the recording and reporting of all current and historical data concerned with each CI. Status accounting maintains records of the current, previous and planned states and attributes of the CIs and tracks these states and attributes: for example, as the status of a CI changes from ''development'' through to ''test,'' ''scheduled to go live,'' ''live,''and through to ''archived.''

Verification consists of a series of reviews and audits to ensure that there is conformity between all CIs and the authorized state of CIs as recorded in the configuration management database (CMDB). It is concerned with checking that the physical CIs actually match the authorized system as described in the CMDB.

5.3.4.2 Network Configuration Management

To ensure the viability of network services the configuration of systems and services must be controlled and managed. Effective configuration management will produce a minimum risk environment.

Configuration management procedures must ensure that details are provided for network equipment and systems covering:

— Configuration activities—how to configure the network equipment

— Security controls

— Access controls

— Configuration history log

— Configuration authority

— Build details

— Fall-back and test records

— Management reporting requirements.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

875 #### 5.3.4.3 Distributed System Configuration Management

876 The services here consist of the following: E

877 — Authentication services for a distributed system environment

878 — Distributed Naming Service Configuration

879 — Distributed Time Service Configuration

880 — X Window system configuration

881 — Window/Session Manager configuration

882 #### 5.3.4.4 Software Installation and Distribution

883 The main types of software to be installed and distributed are application pro-
884 grams developed in-house, bought-in applications, and utility software and per-
885 sonal computer software packages. All software needs to be managed effectively
886 from development or purchase through to the live environment. Unless the distri-
887 bution and implementation process can be controlled automatically, or from the
888 center using software tools, procedures must be in place to ensure that distributed
889 software arrives when expected and is checked for authenticity in whatever way
890 is practical, and that the software is brought into use when required. The main
891 procedures involved in software distribution and installation are:

892 — System management staff at the center to inform remote staff when to E
893 expect distribution software to arrive. E

894 — Recipients to report to system management staff when the distributed E
895 software has arrived successfully. E

896 — System management staff to check that all software is received as expected E
897 at locations. E

898 — System management staff to issue clear instructions about when the E
899 software is to be implemented. E

900 — Location staff to report to system management at the center when the E
901 software has been implemented. The release record on the Configuration E
902 Management Database will state which installations are to receive the
903 release. This database must be updated to reflect the receipt and imple-
904 mentation of the release at each site.

905 #### 5.3.4.5 License Services

906 The terms and conditions relating to the supply of software may place legal res-
907 trictions on the organization (e.g., no unauthorized copies to be made). It is par-
908 ticularly important therefore that the Configuration Management Database is
909 updated with details of who holds copies of software items. This assists the
910 organization in discharging its legal obligations and assists auditors in checking
911 for the existence of unauthorized copies.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

All authorized copies of licensed or purchased software that are made by system E
management staff should be allocated a unique copy number and recorded in the E
Configuration Management Database together with where they are located and
who is responsible for them. Procedural restrictions should be introduced to
prohibit the unauthorized copying of software, and regular software audits should
include a check for any unauthorized copies.

5.3.4.6 Print Output and Distribution Services

Output and distribution packages control output production and distribution from
the moment the output is planned to the time the user receives the print. The
working criteria need to be set up first; e.g., define who receives the report and
how much of the report the user gets.

The main functions are:

— The report can be limited to parts wanted by the user.

— Multiple copies of the entire report, or of selected sections can be produced.

— Reports are grouped by recipient within delivery location.

— Reports for each job are spooled as a group when the job is complete.

— The number of whole reports and individual pages received by each user
are recorded.

— Report production can be monitored and managed efficiently.

Output and Distribution packages should include the following: E

— Printing and distribution of whole and part reports

— Status (queued, printing etc) of the report tracked

— Online viewing of reports

— Ability to archive report files

— Ability to support a wide range of printers

— Costing and charging functionality

— Security facilities

By using an output distribution package, the delivery of reports to the correct per-
son at the correct location can be ensured. Paper, time, and IT resource are saved
as the users receive only the parts of reports that they need, and can also view the
reports online. The number of pages printed can be controlled. Reports can be
tracked from the time they are created to the time they are delivered to the user,
allowing good security monitoring.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

945 #### 5.3.4.7 Office Media Management and Backup/Restore

946 The main services of magnetic tape and data cartridge management systems are: E

947 — Provide automated support for tape housekeeping and maintenance includ-
948 ing:

949 • Allocating tapes and releasing them for reuse helping

950 • To ensure even patterns of use where appropriate

951 • Constructing and triggering cleaning schedules

952 • Maintaining the security of data

953 — Help automate archiving (vault management) for offsite storage

954 — Help identify growth requirements

955 Vault management is concerned with controlling the movement of tape cycles
956 from one storage location to another. As a tape cycle is used, the tape manage-
957 ment system automatically logs a different vault identifier against each tape.

958 A backup strategy is required to control the frequency of backups and the way in
959 which they are created; e.g., whole volumes to cartridge or individual files to tape.

960 The backups and restores of system and application software should be separate
961 from the backups and restores of data. Software and library backups should be
962 explicitly scheduled and the complete software item or library backed up. The
963 schedule for backing up files must be fully documented, properly maintained and
964 adequately safeguarded as the contents of the schedule are required for disaster
965 recovery purposes.

966 #### 5.3.4.8 Online Disk Management

967 The operation of disk management systems requires that they take account of a
968 range of factors such as retention period, recovery, space fragmentation, disk
969 overflow, file and record activity levels, and channel use. Some systems merely
970 report against values or thresholds set, but increasingly they invoke corrective
971 action. Typically, the corrective action is file and disk reorganization or file and
972 data archiving.

973 If a disk management system is used, the constant monitoring and actioning of
974 requests for disk space can be minimized. Disk space may be collectively pooled
975 and unused space constantly reclaimed.

976 #### 5.3.4.9 Job Scheduling

977 Scheduling involves the continuous organization of jobs and processes into the
978 most efficient sequence, maximizing throughput and utilization to meet the tar-
979 gets set in service level agreements (SLA). Jobs are scheduled to ensure:

980 — SLAs and user requirements are met; e.g., certain jobs need to be run by a
981 certain time

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

— Available capacity is used effectively; e.g., the workload run at any given time does not exceed the practical capacity.

The minimum services of a scheduler should include: E

— A high upper limit for the number of relationships allowed between jobs

— The ability to schedule by calendar and criteria

— Workload balancing support

— Levels of security

— Ability to restart jobs

— Operator override capability

— Capability to model future workloads.

5.3.4.10 User Administration E

The services here consist of the ability to: E

— Create a new user or group of users E

— Delete a user or group of users E

— Allocate system resources to a user or a group of users E

5.3.4.11 Accounting

An effective cost management system should contribute to the development of a E
sound investment strategy that recognizes and evaluates the options and flexibil- E
ity available from modern technology. The services here should provide the abil- E
ity to: E

— Establish targets for performance E

— Measure performance against targets E

— Measure and prioritize resource usage E

— Monitor assets and maintain records for control purposes E

— Apportion costs of IT services to users E

— Report costs to management and users E

5.3.4.12 Performance Management

The services here should provide the ability to: E

— Monitor hardware, software, and network performance E

— Monitor workload and throughput E

— Set and adjust system parameters to tune performance E

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

— Monitor terminal response time E

5.3.4.13 Capacity Management

An effective and efficient capacity management function contains at least the following elements:

— Performance management to monitor and optimize the use of current systems.

— A capacity management database that contains current and historic data of technical and business related interest. This database forms the basis for the provision of both tactical and strategic reports on performance and capacity.

— Workload management to identify and understand the applications that make use of the system. The understanding of workloads has both a technical and business related nature. This involves application sizing to accurately predict the performance and required capacity of new applications.

— Capacity planning to accurately plan the required hardware resource and associated cost for the future and to predict the effect on performance and capacity of both tactical and strategic plans.

5.3.4.14 Fault Management E

These services allow the system to react to the loss or incorrect operation of system components at various levels (hardware, logical, services, etc.). The classical model of fault tolerance has a three-step approach. The three steps are fault detection, fault isolation, and fault recovery. Typically implementations divide these steps into multiple steps or integrate them into one or two steps. Additionally, fault diagnosis services support the other steps in the treatment of a fault.

Various fault tolerance strategies, such as checkpointing and voting, are implemented as a collection of services comprising one or more of the steps in the fault tolerance classical model. For example, services involved in implementing a three-node voting scheme will include a vote comparator service (fault detection), vote analyzer service (fault isolation/fault diagnosis), a service to pass the majority ‘‘answer’’ through (fault recovery) as well as a service to disable the faulty resource and reconfigure the voters (fault recovery/reconfiguration).

Fault Detection

Fault detection services are concerned with determining when a fault has occurred in the system. Fault detection services are both passive and active. Active services are those that attempt to determine the status of various system components by testing those components. Passive services, on the other hand, try to ascertain system components by passively gathering information and watching the behavior of the system.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Fault Isolation

Fault isolation services attempt to determine the component at fault and segregate the faulty component from the rest of the system. Services may be shared between the fault detection and isolation service library in that they perform both functions.

Fault Recovery

Fault recovery services attempt to bring the system into a consistent state. These services may be very interrelated to the scheduling services, network services, and data base services, depending on the recovery scheme used.

Redundancy of resources is many times needed to support fault recovery. Resources may include data, process, processor, disk drive, etc.

As parts of the system fail, it may no longer be possible to satisfy all the requirements of the application. Services to support graceful degradation may be used to ensure that critical activities do not fail.

Fault Diagnosis

These services deal with the system's ability to analyze the attributes of a system fault and determine its cause. These services tend to be very interrelated with fault detection and fault isolation services.

Fault Avoidance

These services involve the avoidance of faults before a failure in the system component occurs. If a system can detect that the operation of a component is approaching the edge of its operational range, a standby or backup component could be phased in to replace it. Another form of fault avoidance is logging of shocks, temperature extremes, etc., so that it can be predicted that a component will not meet its original expected service life.

Software Safety

These services involve the system's ability to keep application software from causing harm to the system's software, hardware, or user. For instance, a process may attempt to write into another process's memory space without permission.

A good example of a reliability method that may provide software safety is a bounds checker. The checker compares an answer supplied against the bounds. If it is not within the bounds, the bounds checker will not allow the answer to propagate, possibly causing damage to the system's integrity. Additionally, it may send a fault message (or security violation information, depending on the type of answers expected) to the proper service.

To enhance software safety, other services and processes should be only given the resources necessary to complete their job.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Status of System Components

These services involve the obtrusive and nonobtrusive diagnosis of the state of system components. For further explanation of these services, see Fault Detection and Fault Diagnosis services. These services may additionally need to record and/or display information concerning performance, configuration, and general system information.

Reconfiguration

These services allow the system to reconfigure its view of the world. This services allow the system to substitute different resources to perform system functions such as substituting a new physical I/O channel to support a logical channel. These services are part of the API but their use may be restricted to specially authorized programs such as those used by the target system operator.

Maintainability

Maintainability services provide support for the maintenance of a system. A major component of that support is the collection and logging of information about the operation of the system. Typical information to be logged is:

— Software and hardware errors during operation

— Processes that failed or almost failed to meet scheduled deadlines

— Performance metrics for system tuning

— Times when the system operated in extreme environmental conditions

— Errors reported during startup self-testing

— Attempts to violate rules of the system's security policy.

5.3.4.15 Security Management

— Configuration of appropriate ACLs for System, User Interface, Storage, Network, and application software services.

5.3.5 Standards, Specifications, and Gaps

There are a number of international and national initiatives to develop standards for system management. E E

Note to reviewers: This subclause will be expanded in a later draft. E

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

5.3.6 OSE Cross-Category Services

— Security for remote print jobs

5.3.7 Related Standards

None.

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Section 6: Profiles

Responsibility: Fritz Schulz

This section targets those who want to know more about what profiles are and those who are in the process of developing their own profiles. The latter group consists of those developing formal ''Standardized Profiles'' and those developing less formal profiles for their industry group (e.g., a banking trade association) or their own company or enterprise for procurement or strategic planning purposes.

Those not involved in the development of profiles should read 6.2. Parts of 6.3 also may be useful, especially the earlier subclauses that give definitions of terms and explain concepts more precisely.

Developers of profiles that are not formal POSIX Standardized Profiles (POSIX SPs) should read all of Section 6.

Developers of profiles that are formal POSIX SPs should read all of Section 6 and Annex A.

6.1 Scope

The information presented here about profiles is limited in scope to assist those needing to understand profile concepts as they apply to the POSIX Open System Environment. Covered are profiles constructed from standards (and profiles) listed within this guide (that, by design, are consistent with POSIX.1).

The goal is to create a common approach and documentation scope and style for POSIX-oriented profiles. Annex A goes further by giving specific guidance to developers of formal POSIX SPs.

6.2 Profile Concepts

Responsibility: Bob Gambrel

Introduction

This guide is designed to assist in the selection of standards in the procurement process or as a target application environment. Profiles also assist in the selection of standards. A profile is a suite of base standards with specified options. Profiles can be created by software developers to describe the environment they

Copyright © 1991 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.