Information Network and Data Communication, III, 26-29.3.91, Lillehammer, Norway
D. Khakhar and F. Eliassen (Editors)
Elsevier Science Publishers B.V. (North-Holland)

Network Management in Heterogeneous Networks for Factory Automation

Martin Bosch, Georg Rößler, Werner Schollenberger

Institute of Communications Switching and Data Technics
University of Stuttgart
Stuttgart, Federal Republic of Germany

In factory automation, network management is one of the most important problems of communication, today. Without an effective network management, standardized protocol profiles will not be accepted by the majority of users. Especially, the management of heterogeneous networks is still not treated by standardization committees. This paper describes a Network Management Gateway, which will be a necessary component in future factories, when standardized and proprietary networks have to work together forming one large distributed system.

1. Introduction

The process of integrating all computers and controllers of a company to a large distributed system is in full swing. It will lead to a Computer Integrated Manufacturing (CIM), which is necessary in modern factory automation to react flexibly enough on changes dictated by the market. Besides the material flow, the information flow grows more and more important. This information is usually transmitted via Local Area Networks (LANs). The International Organization for Standardization (ISO) has developed the Basic Reference Model for Open Systems Interconnection (OSI) [2] as a framework for communication protocols. Due to some missing standardized protocols in the application system, various proprietary protocol profiles have been developed. To overcome their incompatibility, Interworking Units (IWUs) are necessary between each pair of communicating LANs. The costs of IWUs are immense and usually they lead to a reduced performance and functionality. Therefore, a standardized protocol profile like the Manufacturing Automation Protocol (MAP) [8] is absolutely necessary in the factory of the future.

At least for a transitional period, the MAP profile, as well as one or more proprietary protocol profiles will be used simultaneously in a company. To overcome the resulting communication barriers, specific IWUs to MAP (*MAP-Gateways*) are necessary. An example for a *MAP-Gateway*, including a performance evaluation, has been presented in [1].

With the growing size, sensitivity and importance of LANs for factory automation, another problem becomes increasingly important: the management of these networks, which will represent the backbone of factory automation in future. This network management becomes more difficult by the heterogenity of networks mentioned above. In a heterogeneous environment specific *Network Management Gateways* are necessary to allow an overall network management by dedicated manager stations.

2. General Aspects of Network Management

2.1. Purpose of Network Management

The primary goal of network management is to guarantee a certain quality of service for the whole network to which the following aspects contribute:

- availability,
- reliability,
- data throughput,
- utilization of the network resources,
- security.

The network to be managed can be regarded as a distributed system consisting of stations and their interconnection paths. Network management disregards the role of a station in the production process and is restricted to its communication resources. The information about these resources relevant for network management is comprised in the term Managed Object (MO). All management operations refer to Managed Objects. Although in open systems the communication protocols are well standardized, the stations themselves remain inhomogeneous resulting in different Managed Objects.
Network management involves

- planning,
- initialization,
- monitoring (recognition of overload situations),
- maintenance,
- fault diagnosis and repair,
- support on configuration changes,
- performance optimization.

It includes human activities and must be individually adapted to each network. Figure 1 shows the general logical structure of network management. It consists of the Network Administrator, usually a human being, a User Interface (Management Console) and the Management System providing a set of services to the Network Administrator and being able to handle some management functions automatically. Today it seems to be impossible for the Management System to cope with all situations occuring in normal operation of the network. An essential aspect of network management is the transfer of management information. This is done by the Management Information Service (MIS).

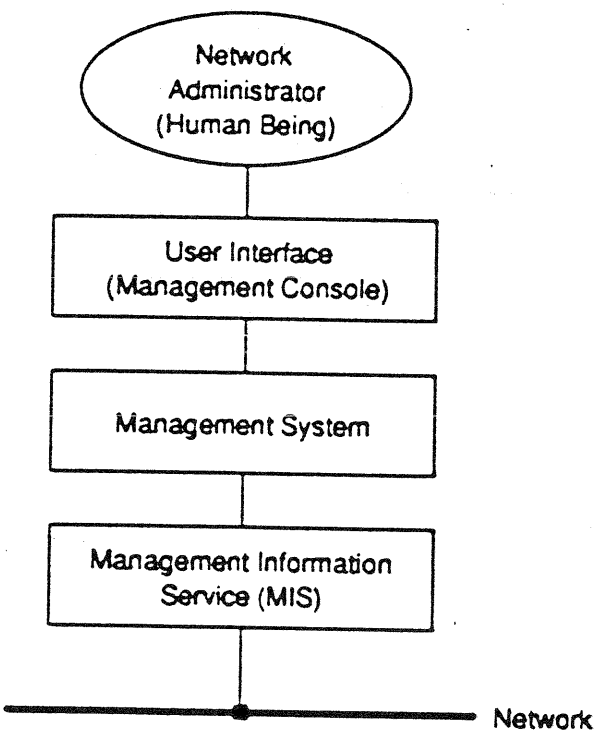

Figure 1 : General Logical Structure

For network management in open systems it is not sufficient to standardize communication services for the exchange of management data, but a common representation and understanding of these data is necessary. In addition, the management system must be

able to perform operations on resources of remote stations in order to assist the Network Administrator efficiently. These issues are the goal of various ISO standardization activities. An abstract model of OSI Management is defined in the OSI Management Framework [3]. Other standards deal with the application layer communication services for network management [4, 5] and the representation of management information [6, 7]. The following section gives a brief overview to the principles and ideas of OSI Management.

2.2. Network Management in OSI

2.2.1. Architecture

Managed Objects are the target of all OSI Management operations. Altogether they form a conceptual database called Management Information Base (MIB). The MIB is distributed over all stations in the network. The location of Managed Objects corresponds to the location of the related resources. A Managed Object consists of

- Attributes,
- Events,
- Actions,
- other Managed Objects being contained in this object.

A Managed Object instance is defined by its name (Object Identifier) and its type (Object Class), which includes the possible operations on it and its attributes as well as all fault situations. Attributes represent values of the related resource which can be read and set by the manager. Events are predefined messages which will be reported from the managed station to the manager in case of relevant state transitions. They are related to attributes. Actions can be initiated in the managed stations. This enables the manager to request an open system to initialize its communication resources, to reset itself or to perform some test functions like echotests to other stations.

A Managed Object can contain further Managed Objects in addition to its attributes, events, and actions. This leads to a hierarchical structure in which the highest level is an object of class SYSTEM representing the whole station. The addressing scheme of Managed Objects is a tree structure, the Containment Tree.

As shown in Figure 2, OSI standardizes three levels of management communication

- (N)-Layer Operation,
- (N)-Layer Management,
- Systems Management.

(N)-Layer Operation provides mechanisms for monitoring and controlling of a single instance of communication via normal (N)-layer protocols between Layer Entities (LEs). (N)-Layer Management addresses several (N)-layer instances and provides mechanisms to monitor and control Managed Objects of one layer. Management operations restricted to layer N can be executed by a (N)-Layer Management Entity (LME) using (N)-Layer Management protocols. The End System to Intermediate System routing exchange protocol for use in conjunction with the protocol providing the connectionless-mode network service (ES/IS Protocol) is an example for a (N)-Layer Management protocol. The most important and powerful mechanism for monitoring and controlling Managed Objects within an open system is Systems Management. It is the only way to manage multiple layers and requires the availability of all seven layers of the protocol stack.

The only instance having access to management data of all layers of one station is the Systems Management Application Process (SMAP). It carries out Systems Management operations and is based on a specific Application Layer Management Service, provided by the Systems Management Application Entity (SMAE) using Systems Management protocols.

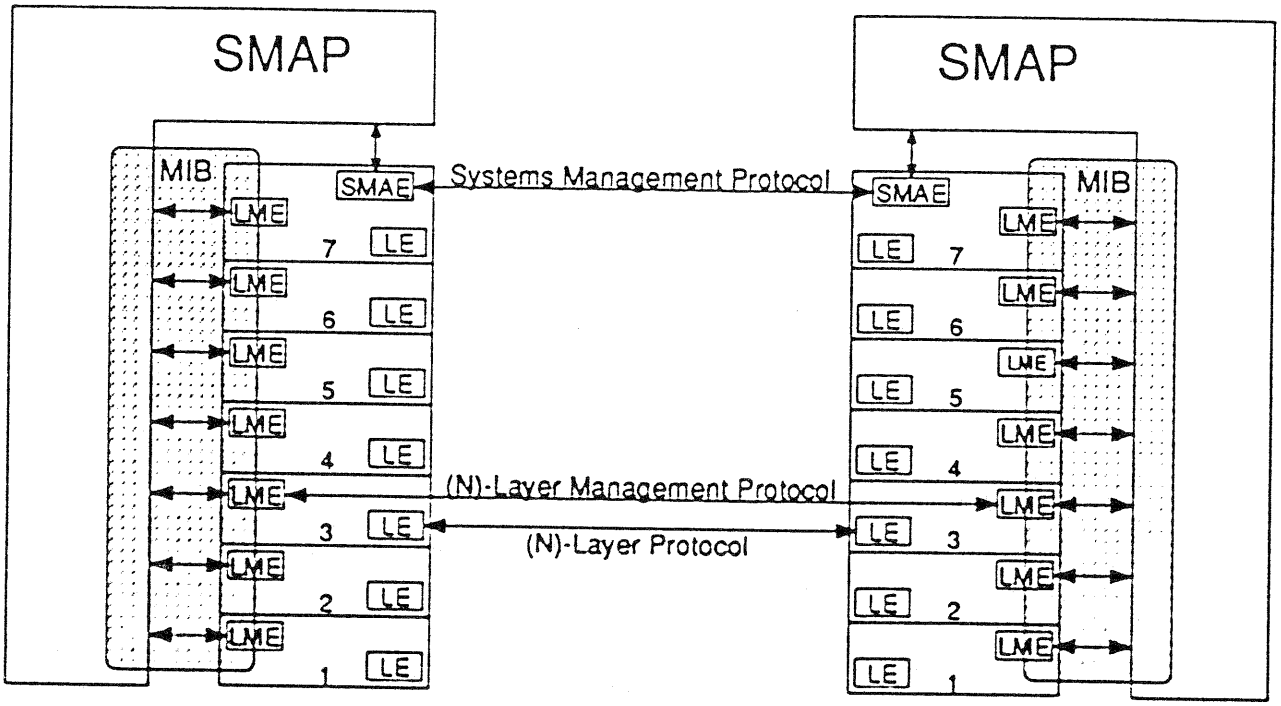

Figure 2 : Communication Model of OSI Management

2.2.2. Systems Management

Individual application processes on individual stations share the task of network management as depicted in Figure 3. They can be divided into manager processes (managers), initiating management activities and agent processes (agents), which have access to local Managed Objects and serve as peer entities for the manager. Every station with full communication capabilities holds one agent responsible for the Managed Objects of this station. Every operation on Managed Objects is invoked by a manager and performed by the agent concerned.

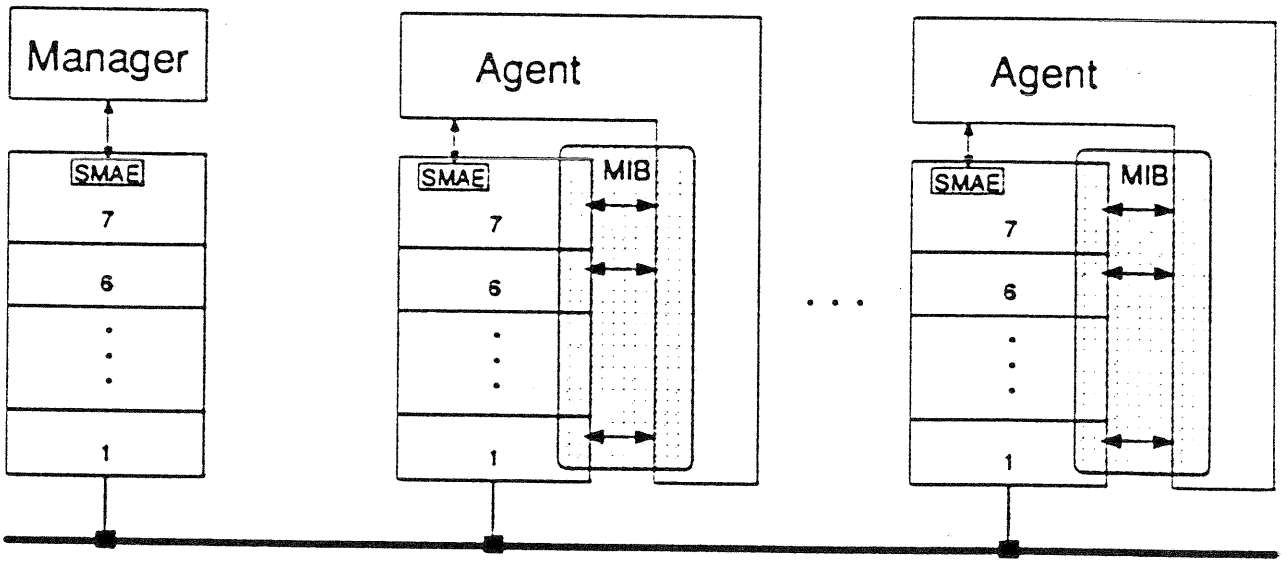

Figure 3 : Manager — Agent Relationship

Figure 4 shows the structure of a SMAE. The communication between managers and agents is performed by the exchange of Management Directives. For this purpose, the application layer provides the SMAE. The interface to the SMAP is realized in the Systems Management Application Service Element (SMASE), which defines a specific set of primitives for each management functional area (refer to subsection 2.2.3.). These primitives can be directly mapped onto primitives of the Common Management Information Service Element (CMISE), which is standardized in [4] together with the related Common Management Information Protocol (CMIP) standardized in [5].

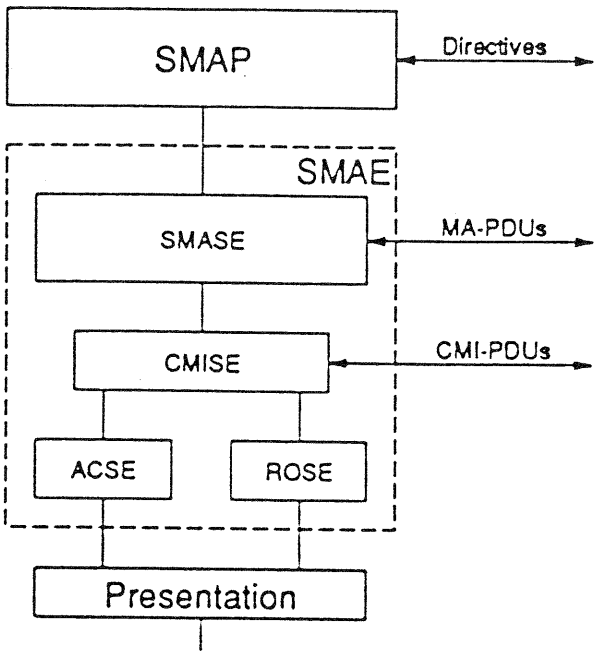

Figure 4 : Structure of the SMAE

The SMASE employs some parameters not used by the CMISE. The CMISE is based on the Application Service Elements ACSE (Association Control Service Element) for the control of CMIS associations and ROSE (Remote Operations Service Element) for the execution of remote operations. CMIS is a connection oriented service. It defines primitives to

- control the establishment and termination of CMIS associations,
- manipulate Managed Objects,
- report on events,
- initiate actions on remote stations.

The complexity of this service is not caused by a large number of service primitives as in the Manufacturing Message Specification (MMS), but by the number of Managed Objects with their individual definitions. For each primitive the CMISE can act as an invoker or as a performer. The role of each communication instance is negotiated during connection establishment. The primitives to control CMIS associations are

- M-INITIALIZE (association establishment),
- M-TERMINATE (normal termination),
- M-ABORT (abnormal termination).

The modification of Managed Objects is usually invoked by the manager and performed by the agent. The primitives to be used are

- M-GET (read one or several attributes),
- M-CANCEL-GET (abort a pending M-GET activity),
- M-SET (change an attribute),
- M-CREATE (create a new incarnation of a Managed Object),
- M-DELETE (delete an incarnation of a Managed Object).

The primitives mentioned above have additional parameters to specify the range of attributes (scope and filtering) and the behavior in case of errors (synchronization). With the scope parameter a set of Managed Objects is selected, which can be the specified object itself, the n-th level below the specified object in the Containment Tree or the whole subtree. The filtering parameter allows the expression of conditions attributes

have to satisfy to get selected. The results of a M-GET request are transmitted via M-GET response primitives. Only the attribute values of one Managed Object can be returned with one Protocol Data Unit (PDU). In case of the selection of multiple objects, several linked response PDUs are transmitted (linked reply).

To inform the manager of certain events in its station, the agent uses the primitive M-EVENT-REPORT, which is related to a Managed Object. The information carried by this PDU depends strongly on the definition of the event.

M-ACTION enables the manager to initiate specific predefined actions in the remote station. The positive acknowledgement of a M-ACTION request indicates only the acceptance by the agent. The results of the action are transmitted in a M-EVENT-REPORT message.

2.2.3. Management Functions

In OSI standardization the different network management requirements are classified into five groups named Specific Management Functional Areas (SMFAs):

- Fault Management,
- Configuration Management,
- Performance Management,
- Security Management,
- Accounting Management.

Fault Management is the set of facilities which enables the detection, isolation and correction of abnormal operation of the network. The functions for Confidence and Diagnostic Testing (CDT) are a subset of these facilities. CDT defines actions to test the connectivity to other stations, e.g. connectivity test (test, whether station A is able to establish a connection to station B), connection saturation test (test, how many connections can be established between stations A and B simultaneously) and data saturation test (determine the maximal data throughput over one connection between stations A and B).

All functions dealing with network configuration as well as the addressing and controlling of Managed Objects refer to Configuration Management. Object Management as a subset of Configuration Management defines functions to get and set attributes of Managed Objects for configuration purposes. The function Enrol Object introduces a new Managed Object to the manager. Since a whole station is represented as one Managed Object of class SYSTEM, Enrol Object allows the introduction of a new station to the manager. On the other hand a Managed Object can be deactivated with the function Deenrol Object.

Performance Management is the set of facilities needed to evaluate the effectiveness of communication activities. They are used to gather statistical data about Managed Objects for planning and analysis purposes. A subset of this function is Workload Monitoring. It defines thresholds for attributes which are supervised by the agent, e.g. the rate of the number of PDUs sent by one layer. Each threshold is related to an event which is reported to the manager if the corresponding attribute exceeds the defined limit.

For the remaining functional areas standardization has just begun, therefore they are rarely implemented today. The facilities of Accounting Management enable charges to be assigned to the usage of Managed Objects. This includes the combination of costs where multiple Managed Objects are involved to provide a special service. Security

Management addresses the protection of information and communication resources from damage and misuse by unauthorized individuals.

3. Interconnection of Heterogeneous Networks

3.1. Principles of Internetworking

In this section it is assumed that the protocol profiles of the networks to be interconnected use identical protocols at and above a specific layer N. The coupling layer of the IWU, as depicted in Figure 5, may then be layer N-1 or above. The protocols of the lower layers 1 to N-1 are independent of each other. The protocols above the IWU's coupling layer have an end–to–end significance.

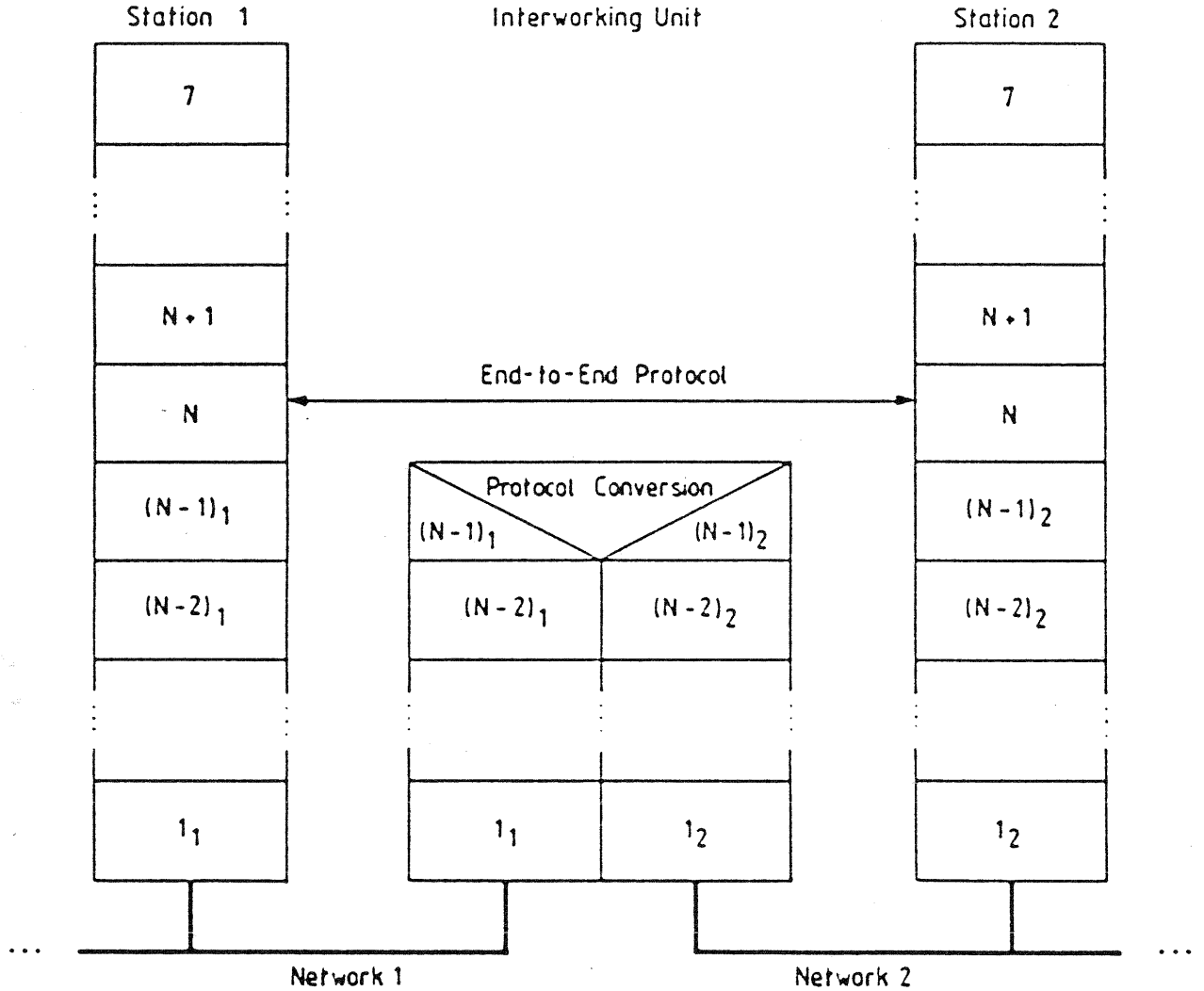

Figure 5 : Internetworking by Protocol Conversion

The networks are usually interconnected at the last different layer N-1 by protocol conversion. The protocol conversion software performs a mapping between service primitives of the two different N-1 protocols in the IWU. Sometimes the lack of a corresponding service primitive in the other protocol can be overcome by adequate sequences of available primitives. The entities of layer N-1 in the IWU may be identical to the corresponding entities in the other stations, respectively. Alternatively a specific layer N-1 entity for the IWU can be used, which performs a direct mapping of PDUs without using service primitives. The advantage of protocol conversion at layer N-1 is the end–to–end protocol at layer N and the minimal number of layers in the IWU, which results in a

minimal transfer time through this device. The existing stations at the interconnected networks 1 and 2 may remain unchanged.

As an alternative to protocol conversion, internetworking may be realized with the help of a global sublayer, by a common protocol in all stations or via transit systems by encapsulation of PDUs.

IWUs may be classified according to their coupling layer. A repeater is a physical layer IWU, which allows an extension of the limited size of a LAN. A bridge interconnects usually LANs on the Media Access Control (MAC) sublayer of the data link layer. On the network layer routers may be used, for example to interconnect LANs via Wide Area Networks (WANs). Internetworking on the transport layer or above is done by gateways.

3.2. Network Management in Heterogeneous Networks

Concerning the network management in a heterogeneous environment, a specific *Network Management Gateway* is necessary besides the IWU necessary for information flow. This *Network Management Gateway* may either be implemented as a dedicated device, or on the same computer as the IWU for the information flow. It should be transparent, so that the manager stations do not become aware of its existence. The concept of having manager stations in each subnetwork will not be considered here, since only one Management Domain is supported in today's manager stations. Additionally, some changes would be necessary in the manager stations implemented according to the OSI philosophy, which contradicts the principle of transparency mentioned above. Instead, we assume to have one or a few manager stations in a standardized OSI compatible network, which will manage the OSI compatible network and the adjacent proprietary networks as well.

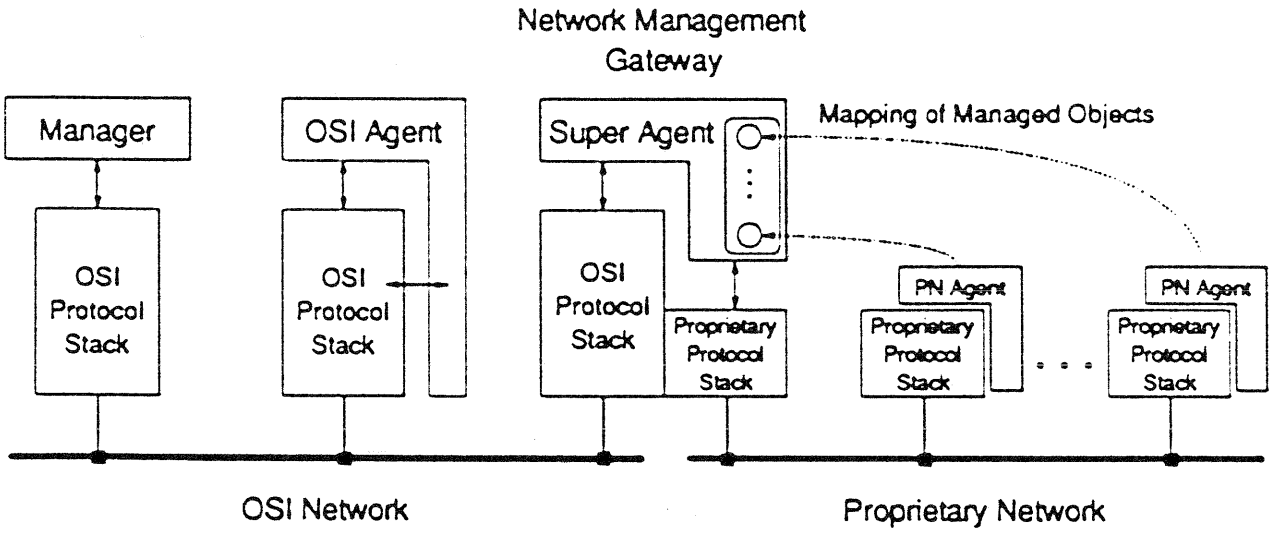

Figure 6 : Network Management via a Network Management Gateway

The *Network Management Gateway* behaves as a manager station from the point of view of its related proprietary stations. Consequently, all proprietary stations must have a Proprietary Network (PN) agent including variables corresponding to Managed Objects, which can be addressed by the *Network Management Gateway*. These variables must be mapped onto Managed Objects or their attributes in the OSI compatible network by the *Network Management Gateway*. As for other IWUs, a loss of functionality can usually not be avoided due to different sets of objects. This mapping can be seen to be located on top of the application layer. The functionality of OSI agents for stations of

the proprietary network is located in the *Network Management Gateway*, as depicted in Figure 6. Therefore, a manager station has to address the *Network Management Gateway* instead of the related proprietary station.

In the *Network Management Gateway* arriving management PDUs have to be converted and then routed to the related PN agent process with the help of an alias address. There are various parameters, which are more or less useful for this routing process. The user information field of the M-INITIALIZE service should not be used as an alias address, to prevent the manager stations from filling this parameter, which would contradict the principle of transparency. In the MAC sublayer the least significant bit of the destination address could be used for alias addressing. With this bit a group address can be indicated. If the *Network Management Gateway* receives all packets with MAC addresses corresponding to the MAC addresses of its related proprietary stations but this bit set to one, the destination address of the target station can easily be determined by an inversion of the least significant bit. The drawback of this addressing scheme is the limited number of allowed group addresses in the *Network Management Gateway* due to the time needed to compare the MAC address of each arriving PDU to all stored group addresses. Another addressing variant is the use of separate Service Access Points (SAPs) at and above an arbitrary layer for each addressed agent. However, this would not be possible at the data link layer in our implementation. In some implementations this would also result in many protocol stacks above the layer where this is done, one for every administered proprietary station. The most adequate addressing concept, however, is the following: One *super agent* in the *Network Management Gateway* contains one Managed Object of class SYSTEM for each related proprietary station. This Managed Object will be addressed directly by a manager and can therefore be considered as the needed alias address. A second agent is responsible for the *Network Management Gateway* itself.

4. Network Management Gateway Design and Implementation

The prototype implementation of the *Network Management Gateway* has been designed to connect two different proprietary networks to an OSI environment for management purposes. In a first phase, the interconnection to one proprietary network has been implemented, the interconnection to the second proprietary network will be done in a second step.

4.1. Protocol Stacks of the Different Networks

Both proprietary networks use an OSI transport system. Therefore, all three networks can share the same physical medium. In the first proprietary network, the transport system is the iNA 960 software on the corresponding communication board from Intel which includes the Network Management Facility (NMF). This NMF consists of a small agent on each system and allows management data exchange based on the transport system. For the layers 1 to 4, attributes, e.g. counters, are defined to achieve network management. In the terminology of the NMF, these attributes are called *NMF objects*. In order not to confound them with the Managed Objects in OSI, these parameters will be called attributes. This convention makes sense, since the *NMF objects* usually represent OSI attributes. The protocol stack above the transport system contains non-OSI protocols and provides no management capabilities. The second proprietary network uses another implementation of the transport system. The higher layers are also different from OSI. On each system in the second proprietary network an agent resides to

exchange management data using a proprietary protocol. In this network, management information is available for all layers of the protocol stack. In Figure 7 the protocol stacks of one manager station in the OSI environment, of the *Network Management Gateway*, and of one station of each proprietary network are depicted as far as they are related to network management.

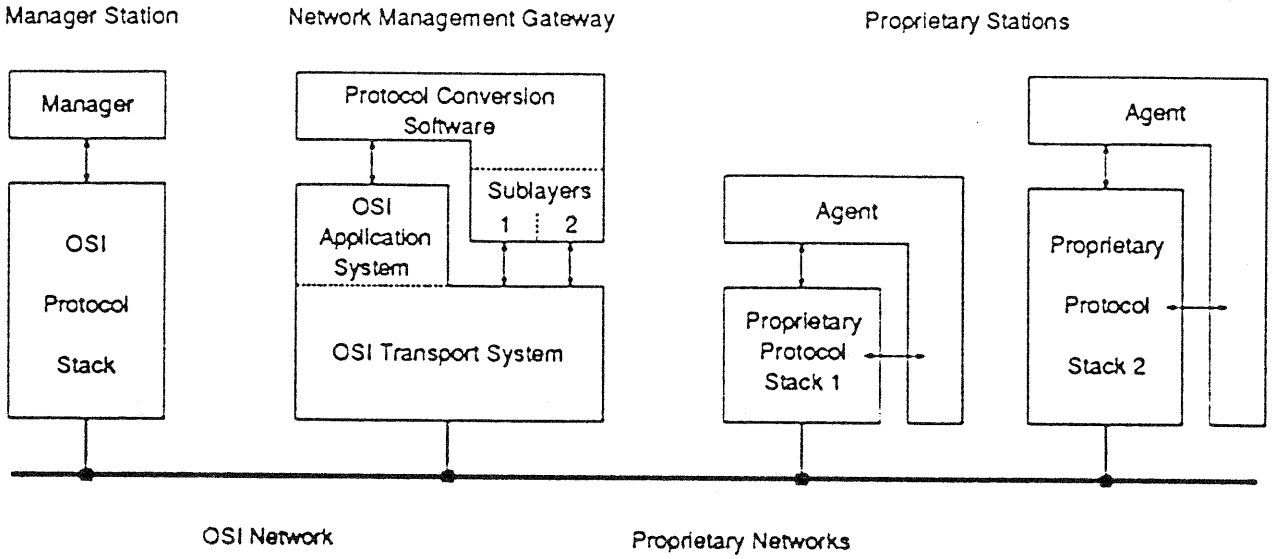

Figure 7 : Protocol Stacks of the Different Networks

4.2. Functionality of the Network Management Gateway

Figure 7 illustrates the functionality of the gateway. The gateway has to convert the CMIS M-GET and M-SET services to the corresponding services in the proprietary networks. Many attributes defined in OSI management are not supported in the proprietary networks but can be stored or calculated using other attributes in the gateway. Examples for these kinds of attributes are thresholds and rates. As the agents in the proprietary networks do not generate event reports, the *Network Management Gateway* has to generate them instantaneously on occurrence of specific events. To recognize these events, the gateway polls several attributes and notifies the manager of irregular or critical workload conditions. The agents in the proprietary networks do not support actions like performing echotests or opening connections for test purposes. The gateway realizes these actions if the results are meaningful to the manager and cannot be misinterpreted.

The gateway must contain both the OSI protocol stack including the CMISE to communicate with the manager and the protocol stacks of the proprietary networks as far as they are necessary for management purposes. Communication in the proprietary networks is based on the common transport system. For each proprietary network, the protocol conversion software contains one sublayer to meet the specific requirements of the networks. On top of these sublayers a common interface for both networks provides a simple and more comfortable access to both proprietary networks. The protocol conversion is done between this interface and that to CMIS.

4.3. Software Structure

As mentioned in section 2.2. network management makes intensive use of data, while the number of service primitives is comparatively small. Therefore, one of the main problems to be solved was to find data structures suitable for both the data contained in the MIB as defined in OSI and the requirements of the proprietary networks. In OSI

management, the data are stored in the Containment Tree in a hierarchical manner. In contrast, the attributes available in the proprietary networks are stored in a kind of linear list with some additional information about the relations between the attributes. These relations are reflected in the numbers employed to identify them. To solve this incompatibility, one hierarchically structured Containment Tree is used with only one Managed Object of each class as a model for all stations in a proprietary network. For each station, the values of all attributes are stored in a data structure containing a few different lists. The model Containment Tree contains no management information but references, where to find the information requested in the data structure. After the protocol conversion software has been started, it reads the necessary information to fill the Containment Tree for each proprietary network from a file. With this method, the relations between the Managed Objects and attributes standardized in OSI and the attributes of the proprietary networks can be modified without changing and recompiling the software.

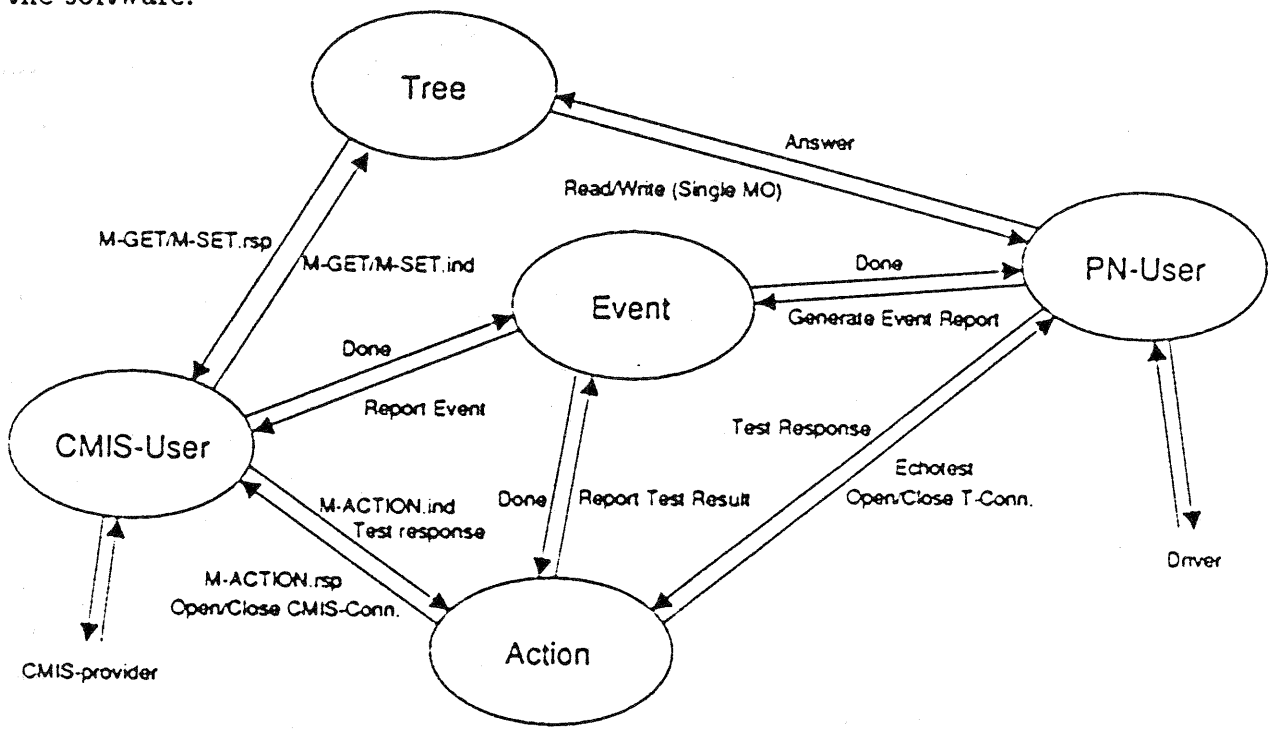

Figure 8 : Protocol Conversion Software Structure

Figure 8 gives an overview of the tasks in the protocol conversion software. The following section describes the functions of the different tasks and the messages they exchange.

The CMIS User Task provides the interface to the OSI protocol stack. The first function of this task is to establish and terminate CMIS associations to communicate with manager stations. Secondly, it enrols each station reporting the Managed Object of class SYSTEM to the managers at the beginning of the management activities. If a station of the proprietary network is shut down, the task deenrols the corresponding SYSTEM Managed Object. The third function is to distribute CMIS PDUs to other tasks to be processed there and to complete the answers of the other tasks to pass them to the CMIS provider.

The Tree Task handles M-GET and M-SET PDUs. It has to evaluate the Managed Objects and attributes from the PDU and has to determine the station and the attributes affected in the proprietary network. To do this, it also processes scope and filter parameters. The treatment of the PDU results in a request to the Proprietary Net-

work User Task containing the operations required and a list of attributes. The answer to this request is employed to complete the corresponding CMIS response PDU. The task generates a linked reply, if multiple Managed Objects are affected. The Tree Task intensively uses the Containment Tree and also the data of the stations to accomplish its function.

The purpose of the Proprietary Network User Task is to provide a simple and comfortable interface for the Tree Task to the proprietary networks. As a normal result of a request from the Tree Task, the task updates the attributes in the station data and returns a list of the updated attributes. Internally, it polls certain attributes if required and supervises the corresponding thresholds. If an attribute value exceeds a threshold, the task notifies this to the Event Task.

The Event Task completes the information received from the Proprietary Network User Task in order to form a CMIS M-EVENT-REPORT PDU. This PDU is passed to the CMIS User Task to be sent to the managers.

The Action Task determines whether the result of the test described in the M-ACTION PDU is meaningful in a heterogeneous environment for the manager stations. If not, it rejects the request, otherwise it initiates the action, e.g. an echotest to a specific station, and activates the Event Task to report the test result to the manager.

4.4. Implementation Aspects

The interconnection software is implemented on an Intel 310 computer with the operating system iRMX II. This operating system is a real time multitasking operating system with priority based preemptive scheduling. The tasks in the system pass data segments to each other via mailboxes. To avoid inconsistencies in the global data used by different tasks, the mechanisms for mutual exclusion provided by the operating system are used. The tasks of the protocol conversion software are implemented in *C* and integrated after a stand-alone test of each task.

5. Conclusion

After an introduction into factory automation, where the necessity of an overall network management can be recognized, we have described the current state of network management and its philosophy in standardization. Specific problems of heterogeneous networks have been summarized. The main focus of this paper has been a *Network Management Gateway* for factory automation. The development of this gateway has been supported by the Commission of the European Communities (CEC) within the framework of the project *Communications Network for Manufacturing Applications* (CNMA), which is a part of the European Strategic Program for Research and Development in Information Technology (ESPRIT). The *Network Management Gateway* extends the management of the standardized CNMA network to stations in a proprietary network. We have described its protocol architecture and functionality as well as the resulting protocol conversion software structure. This gateway will be demonstrated at the University of Stuttgart in the experimental pilot of the CNMA project.

Acknowledgement

The authors would like to thank all the students who have been involved in the implementation of the *Network Management Gateway*.

References

[1] Martin Bosch; "Design, Implementation, Modelling and Simulation of a MAP-Gateway for Flexible Manufacturing", Modelling the Innovation: Communications, Automation and Information Systems, Rome, March 21 - 23, 1990

[2] ISO 7498; "Information Processing Systems — Open Systems Interconnection — Basic Reference Model", November 1983

[3] ISO 7498-4; "Information Processing Systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management Framework", January 1988

[4] ISO DIS 9595-2; "Information Processing Systems — Open Systems Interconnection — Management Information Service Definition — Part 2: Common Management Information Service", 1989

[5] ISO DIS 9596-2 "Information Processing Systems — Open Systems Interconnection — Management Information Protocol — Part 2: Common Management Information Protocol", 1989

[6] ISO DP 10040; "Information Processing Systems — Open Systems Interconnection — Systems Management Overview", 1989

[7] ISO DP 10165; "Information Processing Systems — Open Systems Interconnection — Structure of Management Information", 1989

[8] MAP; "Manufacturing Automation Protocol", Version 3.0, General Motors, Warren/Michigan, April 7, 1987