



NAFEM Data Protocol User Manual

Version 2.00

November 2003

TABLE OF CONTENTS

Figure 1 – The On-line Kitchen Schematic.....4

Overview.....4

 Administrative Enterprise Groups.....5

 Application Enterprise Groups.....5

Terminology.....6

Recommended Equipment Types.....7

Units of Measure.....7

Version and Source.....8

Case Study.....8

Participation.....9

Certification.....9

Compliance and Legalities.....10

Governing Groups.....10

Disclaimer.....10

Enterprise Groups.....11

Administration Enterprise Groups.....11

 Administration Object... ..11

 Clock Calendar Object.....12

 Asset Management Object.....12

Application Enterprise Groups.....	12
Monitor Object.....	12
Maintenance Object.....	12
Utility Management Object.....	13
Inventory Management Object.....	14
Notification Object.....	15
Bulk Transfer Object.....	15
Security Object.....	16

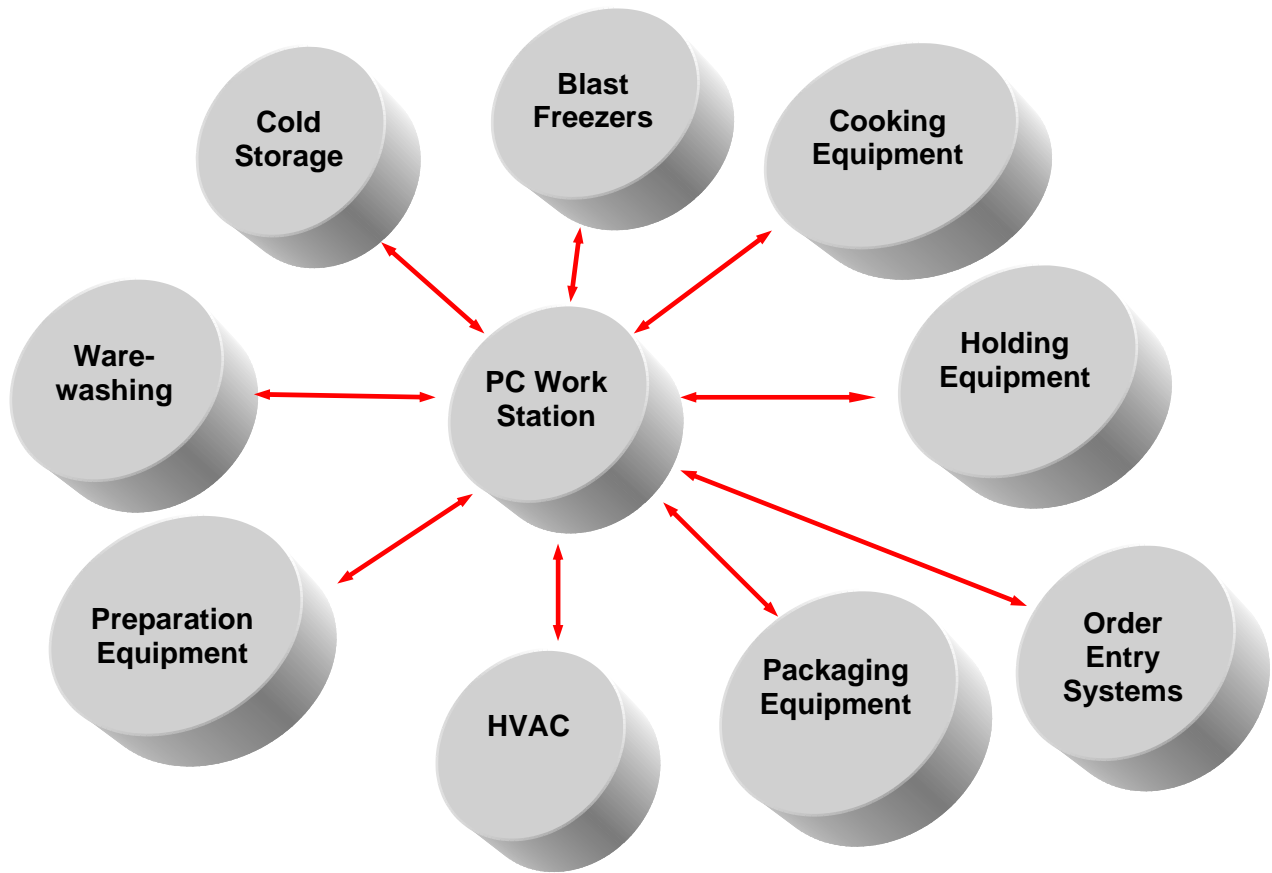


Figure 1 - The On-line Kitchen Schematic

OVERVIEW

The on-line kitchen is designed to make today's foodservice facilities easier and simpler to operate by automating the management processes for inventory, labor, food safety, asset management, energy consumption and administrative functions.

Major U.S. restaurant chains, anticipating that a lack of prompt and centralized action would result in a variety of independent protocols, encouraged NAFEM to lead the effort to develop an industry-wide set of rules, or protocol, to govern the exchange of data between independent pieces of commercial equipment and a computer.

In response, NAFEM created the NAFEM Data Protocol (NDP), a Standard based on existing, open Internet Protocols (IP).

The NDP is a standard, non-proprietary technology protocol that enables bi-directional communication of data between a central PC-based workstation and foodservice equipment.

Using the NDP to automate management processes benefits owner/operators, food equipment manufacturers and employees. Automating certain functions helps minimize unnecessary steps and simplify processes. Foodservice facility owners and operators can maximize productivity by improving job quality and making the workday more rewarding for employees. Maintenance and service schedules may be automated to create troubleshooting and diagnostic capabilities, which in turn reduces expensive, unplanned downtime.

By using NDP, manufacturers gain the ability to allocate research and development resources to other products and services. As a whole, the industry gains the ability to monitor trends, collect information and provide equipment solutions to increase operational efficiency.

The essential framework of the NDP consists of several building blocks called Enterprise Groups that identify specific functions and information related to the exchange of data such as:

- Format
- Method and content of communication
- Recipient(s)
- Timing and frequency

These Enterprise Groups are separated into two categories – Administration Enterprise Groups and Application Enterprise Groups. The former are mandatory, while the latter are optional.

Administration Enterprise Groups include:

- **Administration:** Identifies the piece of equipment to the network.
- **Clock Calendar:** Enables scheduling functions by tracking current date and time of day.
- **Asset Management:** Maintains specific records for each piece of equipment, such as model number, serial number, manufacturing date, and controller software version.

Application Enterprise Groups include:

- **Monitor:** Defines the criteria the operator wishes to measure/monitor, such as cook and hold times and temperatures, beverage dispensing system flow and volume rates, as well as safety-related information to meet HACCP requirements. Other criteria may be related to equipment performance such as compressor run-time, cook cycle and abnormal operating conditions.
- **Maintenance:** Defines maintenance related to operating parameters and schedules equipment preventative maintenance and cleaning based on usage and performance data. Uses pre-determined operating parameters to detect performance degradation and trigger warning messages.
- **Utility Management:** Assists management of energy costs by defining, monitoring and collecting utility related information. Uses pre-determined utility parameters to detect performance degradation and trigger warning messages.
- **Inventory Management:** Defines inventory items to be monitored, and establishes criteria such as consumption rates, stocking levels, re-order levels and hold times.
- **Notification:** Defines notification parameters such as where messages are sent, frequency and time interval between messages, and keeps a record of messages sent.
- **Bulk Transfer:** Enables managers to send large packets of information between the manager's computer and equipment on the network. Defines storage media type, size and location and establishes data collection and transfer parameters.
- **Security:** Establishes the system parameters that allow registered users varying levels of access to operate the system. Defines which pieces of equipment receive security monitoring and tampering criteria.

TERMINOLOGY

The following definitions may be helpful when reading this Users Manual.

API (Application Programming Interface): A set of routines that an application (software program) uses to interface with lower-level operating system services.

Bridge: A network device that connects two networks that use the same protocol. The bridge forwards packets between the networks, if necessary. Also see gateway.

Behavior: A consistent process that generates a known outcome. Having consistent behavior is a good thing.

Client: A program or device that requests services from a server. The foodservice facility manager's workstation is an example of a client.

Client/Server: A style of computing that allows work to be distributed across different computers or controllers. For example, a PC client can request temperature readings from a controller server to determine if the unit functions correctly. Also see client and server.

Ethernet: A LAN technology that uses packets. Ethernet can run over various types of media, including twisted pair (10BaseT or 100BaseT) as well as wireless (802.11, all versions). Also see LAN and packets.

Ethernet Address: This is a number that uniquely identifies a machine on the network and allows routing of packets to the correct recipient.

Event: A single occurrence that has a distinct beginning and end. Events are not ongoing so the system will not continually send alarm messages. Messages are only sent when a transition from one state to the next occurs.

FTP (File Transfer Protocol): A subset of the Ethernet protocol that allows transferring large amounts of data as files. Some form of authentication may be required.

Gateway: A network device that connects two networks that use different protocols. The gateway forwards packets between the networks, if necessary. Also see bridge.

IEEE (Institute of Electrical and Electronics Engineers): A group of scientists and engineers that advises on standards for ANSI (American National Standards Institute). The IEEE provides oversight for standards governing LANs and Ethernet.

Interoperability: The capability of computers or controllers from different vendors to cooperate and communicate together. For example, a Macintosh computer can share files that are on a UNIX machine.

LAN (Local Area Network): A network that spans small distances, for example between computers in an office. Ethernet is a well-known example of LAN technology.

Packet: Pieces of information that are transmitted over a network to convey a message. Several packets may be reconstructed at the receiving end and ultimately decoded into the original message.

Server: A program or device that provides services to clients on a network. A controller reporting various process temperatures is an example of a server.

SNMP (Simple Network Management Protocol): A subset of the Ethernet protocol used by computers (or controllers) that monitor network activity and performance, to communicate with one another, and the equipment devices that are being monitored.

Trap: An unsolicited message that is generated when an alarm is triggered by an event, resulting from the behavior of an object within the Protocol.

RECOMMENDED EQUIPMENT TYPES

The NDP includes provisions for identifying the type of equipment that is located at a specific address of the network. NAFEM recommends the following listed types of equipment be used. The field used to identify the equipment type cannot exceed 32 characters, including spaces.

<u>Equipment Type</u>	<u>Characters</u>	<u>Equipment Type</u>	<u>Characters</u>
Dispensing	10	Refrigeration	13
Food Preparation	16	Security System	16
Frozen Desserts and Beverages	25	Steamers	8
Fryer	5	Temperature Measurement	23
Griddles/Grills	15	Timers	6
Holding Cabinets	16	Toasters	8
Hot Beverages	13	Ventilation	11
HVAC	4	Warewashing	11
Ice Equipment	13	Waste Systems	13
Ovens	5	Weighing	8
Point of Sale	13		

UNITS OF MEASURE

The NDP includes a table defining units of measure that may be used in conjunction with the protocol. Each unit of measure is identified with a three digit numeric code. Also included are a series of codes reserved for future use and a series of code that are user definable.

<u>Code</u>	<u>Unit of Measure</u>	<u>Code</u>	<u>Unit of Measure</u>	<u>Code</u>	<u>Unit of Measure</u>
001	meter	006	ampere	011	lumen
002	millimeter	007	milliampere	012	lux
003	gram	008	kelvin	013	hertz
004	kilogram	009	celsius	014	newton
005	second	010	candela	015	pascal

Units of Measure continued

<u>Code</u>	<u>Unit of Measure</u>	<u>Code</u>	<u>Unit of Measure</u>	<u>Code</u>	<u>Unit of Measure</u>
016	joule	024	katal	032	psi
017	watt	025	poiseuille	033	btu
018	volt	026	rayl	034	piece
019	ohm	027	dB	035	no value
020	radian	028	inch	036	logic element
021	degree	029	foot	037-599	reserved
022	gray	030	pound	600-999	user definable
023	sievert	031	fahrenheit		

VERSION AND SOURCE

This document is intended to present the MIBs in an easy to use format and is based on version 2.00 of the MIBs, published by NAFEM in June 2003. The only authorized source for the current version is the NAFEM website at www.nafem.org. If MIBs or any other documents are received from any other source, check with information posted on the Web site for updates.

CASE STUDY

Here's one simple example of how a foodservice operation can use the NAFEM Data Protocol.

Your foodservice facility has recently installed a NAFEM Data Protocol compliant system that permits bi-directional communication between each piece of kitchen equipment and a central computer workstation in the manager's office. The communication system also includes Internet access via dial-up telephone connection.

The new system includes mandatory management information bases (MIBs) including asset management, clock/calendar, NAFEM units of measure, NAFEM textual convention and NAFEM traps that were installed in addition to a number of optional MIBs.

The system also includes a few existing pieces of equipment that already include communication capability. These pieces were connected to the entire system using bolt-on communication modules and sensors designed specifically for such applications.

During initial start-up of the system, basic equipment information such as manufacturer name, model number, serial number, operating parameters, electrical/mechanical utility information and local service agency was entered into the system database. Other general information such as date, time of day, location coordinates (longitude and latitude) and the operating schedule for the facility was also entered into the database.

One of the older pieces of equipment is a walk-in cooler. Using the monitor MIB, operating information such as evaporator inlet and outlet temperatures, compartment air temperature, compressor temperature and pressures and compressor cycles are collected. Using the bulk transfer MIB, the raw data is transmitted to the manager's workstation.

Using algorithms included in the system, the raw data is compared with normal operating parameter information entered at system start-up. Upon analysis of the data, the system notes that the condensing unit is running about 30 degrees hotter and it is drawing about 10 percent more current than it should under normal operating conditions.

In addition the evaporator inlet and outlet temperatures are running about eight degrees too warm. To confirm that the abnormal operating data is accurate, the workstation sends a command back to the controller on the walk-in cooler and requests additional data from the sensors on the compressor. Upon confirmation that the data is accurate, a warning message is sent to the manager via e-mail. Simultaneously, an e-mail message is sent to the local service agency advising that there is a problem with the walk-in cooler's compressor.

Using the data provided, the service agency is able to quickly diagnose the problem. Based on the actual operating temperatures and current draw, the service agent determines that the compressor will probably fail within the next five days. The service agency calls the unit manager and schedules a service call to replace the failing part during the mid-afternoon slow period within the next two days.

PARTICIPATION

All manufacturers are eligible to review the NDP materials, download MIBs, complete the registration process and self-certify equipment as NDP Compliant. Once registration is complete, applicants receive notification and approval to market each registered product as NAFEM Data Protocol Compliant®. A database of NDP Compliant equipment is available on the NAFEM Web site and compliance may be promoted through the use of the NAFEM Data Protocol Compliant mark.



CERTIFICATION

Manufacturers desiring to register products as NAFEM Data Protocol Compliant, only need to visit the NAFEM Web site at www.nafem.org and follow four simple steps:

- Register as a user
- Select the NAFEM member company profile from the list provided on the NAFEM website or add a company profile
- Complete the “Declaration of Conformity” and “I Agree” Statement certifying that the product(s) being registered are in compliance with the NAFEM Data Protocol Standard
- Register individual products that are compliant by providing the model number, product, standard with which it complies and any supporting documentation demonstrating compliance.

COMPLIANCE AND LEGALITIES

By completing the Declaration of Conformity and “I Agree” Statement, manufacturers agree to comply with all aspects of the NAFEM Data Protocol Standard and are granted permission to use the NAFEM Data Protocol Certification Mark in conjunction with the registered product(s).

NAFEM reserves the right to limit or revoke use of the Certification Mark if the user or product(s) fail to meet the NAFEM Data Protocol Standard at any time.

GOVERNING GROUPS

The NAFEM Data Protocol Steering Committee, a subcommittee of the NAFEM Technical Liaison Committee, is responsible for ongoing maintenance and industry education related to the NAFEM Data Protocol. In its role, the Steering Committee is responsible for publishing protocol revisions and updates, and providing education and tools to develop understanding and use of the protocol.

Any action taken or recommended by the Steering Committee is subject to confirmation by the Technical Liaison Committee and NAFEM Board of Directors.

DISCLAIMER

Copyright © 2003 North American Association of Food Equipment Manufacturers (NAFEM). All rights reserved. Reproduction of this document is authorized on the condition that the foregoing copyright notice is included.

This SNMP MIB Module (Specification) embodies NAFEM’s proprietary intellectual property. NAFEM retains all title and ownership in the Specification, including any revisions.

NAFEM grants all interested parties a non-exclusive license to use and distribute an unmodified copy of this Specification in connection with the management of products that incorporate the NAFEM Data Protocol, and without fee, provided this copyright notice and license appear on all copies.

This Specification is supplied “AS IS” and NAFEM makes no warranty, either expressed or implied, as to the use, operation, condition, or performance of the Specification.

While we encourage users to incorporate the entire protocol, it should be noted that some Enterprise Groups are optional while others are mandatory. Compliance Registration is maintained by NAFEM and is required to use the registered trademark. Compliance is outlined in this Users Manual and may be found on the NAFEM Web site at www.nafem.org.

ENTERPRISE GROUPS

As already noted, the enterprise groups, also known as objects, are divided into two categories: administration and application.

Administration objects are mandatory and are used to identify a device to the network to which it is connected, scheduling functions and information record keeping used in the management of each piece of equipment connect to the network.

The use of application objects is optional at the discretion of the user. Application objects provide specific functions within an NDP compliant network.

ADMINISTRATION ENTERPRISE GROUPS

Administration Object

Introduction: The Administration Enterprise Group provides a means to track and administer NDP Compliant equipment or devices on the network. The Enterprise Group addresses key network management issues including: Identification (textual and network), authority and enterprise notification. NAFEM Data Protocol compliance requires the implementation of the Identification group of attributes.

Textual identification provides a human readable way to describe the device name, implementation version and manufacturer. This is required to uniquely identify each device, its manufacturer, and the version of NDP Compliance.

Network identification provides a machine-readable way for each device to report network addresses to management hosts. This is required to uniquely identify each device on the network. Identification includes IP address, default gateway, and subnet mask.

Authority provides the means to administer categories or communities of users. This feature allows a device to restrict access to specific user groups based on their access authority. Enterprise notification provides an automatic method to inform the enterprise that the device is on-line and available for interaction or use. This is a network friendly means for each piece of equipment to report its status and availability without the enterprise having to continually poll all devices.

Discussion: In a typical scenario the equipment manufacturer embeds the textual identification information in each unique device. At installation, the textual identification may be modified or augmented. Upon connecting to the network, either automatic or manual network identification occurs. If the enterprise requires different access levels to various groups of users, the authority attributes are implemented.

During foodservice operation, equipment can be taken on and off-line for various reasons. In these situations enterprise notification is a valuable tool. By enabling this service the device can self-report its availability to the network. This is particularly useful when equipment goes into service and minimizes network traffic.

Clock Calendar Object

Introduction: The Clock Calendar Enterprise Group provides for consistent time, date, and scheduling formats needed to accomplish a variety of foodservice management applications. It consists of three functional groups: Time, Daylight and Scheduler.

Time provides access to the current date and time relative to the correct time zone. Daylight provides a method for equipment to automatically adjust for daylight savings time. Scheduler is a tool to allow the scheduling of events.

Discussion: Use Time to time stamp data elements for networked devices to determine when events occur. Daylight allows equipment to automatically adjust for daylight savings changes. This eliminates the task of twice per calendar year, manually updating this data for each item of networked equipment. Scheduler can be used to optimize operating conditions for predictable peak and off-peak demand.

Asset Management Object

Introduction: The Asset Management Enterprise Group provides a means to make nameplate data available electronically. Data can be recorded for both the equipment as well as key components. These data elements include manufacturer, type of equipment, serial number, model number, date of manufacture, date of installation, software version, NAFEM version, contact information, and component part data. Component part information includes manufacturer, device name, serial number, model number, version number, and contact information.

Discussion: In a typical scenario nameplate information is made available to the network for the purposes of tracking and managing equipment assets. For example this data could be used to locate units for: software upgrades, recall issues, installation dates for warranty purposes, and contacts for support and service.

APPLICATION ENTERPRISE GROUPS

Monitor Object

Introduction: The Monitor Enterprise Group provides a means to monitor, log, and report alarms for key operating conditions. High and low alarm limits may be set and management notified when exceeded. Operating conditions can be described and viewed in a human readable form. Data can be time stamped and logged for future database analysis.

Discussion: In a typical scenario the Monitor Enterprise Group could be used for remote and automatic HACCP data monitoring and logging. In addition to HACCP data, many other types of operating conditions could be monitored, alarmed, and logged. Monitoring can occur across any or all NAFEM Data Protocol Compliant equipment connected to the network.

Maintenance Object

Introduction: The Maintenance Enterprise Group can be used to monitor specific equipment parameters that provide information on the condition and status of serviceable components and

trigger corrective service actions such as cleaning, fluid changing or filter replacement. Three types of maintenance monitoring items are provided. Process initiated events such as temperature and pressures or power variation. Counter initiated events such as switch counts, dispense cycles, or use counts. And timed initiated events such as hours, days and weeks of usage are made available by this enterprise group.

Descriptions of maintenance items are entered into a configuration table for each of the types of monitored items. Name, units, equipment type and its location are the description items made available by this table.

Each maintenance item can be configured to signal maintenance events by setting trip levels appropriate for the monitoring type. Setting maximum run time in hours for compressors, replacement notification on air filters by measuring differential pressures across the filter, and/or 100,000 switch closures for relay contacts are examples of these limit setting attributes.

Optionally, the maintenance enterprise group provides network notification services as well as history logging of the monitored maintenance parameters

Discussion: A Kitchen has multiple refrigeration units that require routine cleaning of the evaporator coils to optimize the efficiency of the units. These coils require cleaning every 100 hours that the compressor runs. In addition, the compressor temperature exceeding its nominal operation range is another signal that cleaning is required. With the Maintenance Enterprise group, the refrigeration units are entered and described in the configuration table. The compressor running times and temperatures limits are added so monitoring occurs.

Once the compressor run times exceed 100 hours or its temperatures exceed nominal range, a notification is sent to service personnel for corrective action as well as a record being stored for each piece of equipment and maintenance event.

Utility Management Object

Introduction: Utilities are the external power sources and plumbing connections supplied to the equipment such as electric, gas, water, steam, etc. The Utility Object permits the operator to enter equipment utility operating parameters for comparison to actual operating data. This object consists of four tables including:

- Utility Management Configuration Table
- Utility Management Data Table
- Utility Management Alarm Table
- Utility Management Log Table
- Utility Management Log History Table

The Utility Management Configuration Table defines what utility information is to be monitored and includes the type and description of the utility, the rated value of the utility and the unit of measure.

The Utility Management Data Table is the actual information being recorded and includes utility values within the equipment that are to be monitored, the actual data entry, an index code of utility type, unit of measure, status and time and date stamp.

The Utility Management Alarm Table is the triggering mechanism for sending alarm (traps) messages. Included are an index, critical high and low limits, high and low alarm warning limits, deviation parameters as well as alarm clear or by-pass commands.

The Utility Management Log Table defines how logging is performed. There is one entry for each utility type. In addition, logging may be selectively activated.

The Utility Management Log History Table is the raw historical data collected.

Discussion: In a beverage dispensing system, a minimum incoming water pressure must be maintained. In the event the in-line water filtration system becomes clogged, the water pressure drops below the minimum operating parameter and an event is logged in the data table and an alarm notification is sent to the operator.

An oven that suddenly has a significant reduction in power consumption may be characteristic of a failed heating element. An event is logged in the data table and an alarm message is sent to the operator.

Inventory Management Object

Introduction: The Inventory Management Enterprise Group is used to ensure a kitchen is always stocked with the appropriate amount of inventory necessary to satisfy current and forecasted supply and provides status and management of current production and demand levels. The Inventory Management group helps answer the question “Can I satisfy my customers’ demand?”

Each inventory item is defined within a configuration table that allows for item naming, description, and measurement units along with vendor identification and product codes. These entries provide simple means to uniquely identify product or ingredients.

During the processing period, each inventory item is monitored for current usage and total consumption. Each item’s data value has a time stamp to determine the time of day and day of year it was consumed or produced. This information can be recorded using the logging feature to develop usage trends and provide input to forecasting or consumption modeling for the facility.

Individual thresholds can be assigned to trigger notification of pending storage or excess demand. Using notification services provided by Enterprise Group, these events could be communicated to message centers for immediate action by the store personnel.

Discussion: Assume that your operation would like to develop a consumption model for usage of steak sandwiches. The ingredients are entered through a PC application connected to your NAFEM enabled equipment into the configuration table portion of inventory management group. As each steak patty is produced, a totaling value is generated along with a logged record of each batch of patties produced.

The host computer system reads these logged entries from your NAFEM enabled equipment and inputs them into a consumption modeling algorithm, thereby forecasting future demand and determining future steak patty order quantities.

During this processing period the produced number of steak patties begins to exceed the on hand quantity [items at the grill] and notifies the personnel via a message from your NAFEM enabled equipment to the back office PC. The personnel then proceeds to remove more patties from the walk in cooler to replenish the local inventory at the grill.

This process can be repeated for other inventory items such as beverages, disposable packaging and even labor.

Notification Object

Introduction: In the course of day-to-day operations, events occur that the operator may choose to have recorded for later analysis. Other events may require immediate operator attention. This object defines how those events are logged and to whom notification is sent. Other objects define which events are logged. This object serves as the address book for those other objects. The Notification Object consists of three tables:

- Notification Host IP Table
- Notification Event Log Configuration Table
- Notification Event Log Table

The Notification Host IP Table includes four elements: an index of entries, name of the host(s) to be notified, the IP address for each host and a listing of Host IP Groups. The name of the host is the addressee for the messages that are human readable. The IP address is the addressee for the messages that are machine readable.

The Notification Event Log Configuration Table defines how the event log will be configured. Elements include the name of log file, the size of the log file, the number of days the entry will be saved before being overwritten and a clear table command.

The Notification Event Log Table is the actual listing of events. The event log includes an index, the date and time of the event, the name of the event, the event log group, the actual event message, event code and any other details that may be required to define the event.

Discussion: For an example, if during operation, a piece of cooking equipment begins operating below its minimum temperature. The object initiating the event would use this object to determine to whom notification is to be sent. An entry into the event log would be made and notification and description of the event may be sent to the operator.

Other examples such as number of batches of product cooked, batch size, cook time, hold time are also events that, at operator discretion may be logged to the Event Log Table. Such data may be for later review or analysis or may be tied to real-time inventory control.

Bulk Transfer Object

Introduction: In every day operation, it may be necessary, to collect and hold lower level, non-critical data locally and then transmit the data in bulk during a period of low activity on the network. The Bulk Transfer Enterprise Group permits this function within a NAFEM Data Protocol Compliant network.

Various tables identify the data to be held, how long the data is to be held, the transfer destination, whether or not an acknowledgment is required and the frequency and interval for transmission.

Discussion: During normal operation, equipment in a foodservice facility cycles on and off on a regular basis. Cycle information is logged in a data table and is held until the unit has closed for the day. The device, sensing that the normal operational traffic on the network has transitioned to a non-operational period, transmits the bulk data in a packet to the manager's workstation.

In the case of a new menu item being added, the new recipe is bulk transferred to the piece of cooking equipment on a predetermined day, prior to the unit opening for the day. Since receipt of the recipe is critical, an acknowledgement is required. Upon receipt of the recipe, the device sends a message back to the host acknowledging receipt of the data packet.

Security Object

Introduction: The Security Enterprise Group provides security and security related functions for access to the network and access to equipment on the network. Security data items may be configured in a variety of ways tailored to the foodservice operation.

User access information including user names, access passwords, level of access and tamper criteria are entered into configuration data tables. Security items to be monitored are entered into a Security Item Monitor Data Table. Log tables monitor entries into the various data tables.

In an operating NAFEM Data Protocol Compliant network, access to recipe settings on cooking and holding equipment is restricted to the unit manager and upper level corporate operations staff. In order to reprogram or change any equipment setting or program, an access code must be entered. Unauthorized attempts to access equipment or restricted files results in a notification message being generated and transmitted to predetermined locations.

Discussion: A new item is being added to a restaurant chain's menu. Prior to rolling out the new item, a cooking recipe must be added to a piece of cooking equipment system wide. A systems programmer in the corporate headquarters has written the program code for the recipe and, using a global access code and an internet connection to each unit, down loads the recipe to the manager's workstation in each unit. On the day the new menu item is to be added, the manager's workstation downloads the new recipe to the piece of cooking equipment.