PEER REVIEW PAPER

Computerized Maintenance Management Systems

Ted Cohen
University of California Davis Health System
Sacramento CA
Nicholas Cram
St. Joseph Regional Health Center
Bryan TX

How do clinical engineers (CE) ensure that the medical systems installed in their customers' healthcare organizations are functioning optimally? What do they do when those medical systems malfunction? What is the quickest route to restoring performance of the medical system to the customer's satisfaction, and at what cost? How do they help determine when to replace a major system? How do they interact with the healthcare providers and all the other "customers" in a modern, complex, healthcare organization such as accrediting organizations, FDA, device manufacturers, risk managers and attorneys. Most use some type of computerized record-keeping system to help manage their business.

Computerized Maintenance Management Systems (CMMS) have evolved into a key tool in providing technology support. Whether supporting a three-technician shop or an international service organization almost all medical equipment support organizations are using some type of CMMS in their operations. These CMMS's can be broadly classified as internally developed (typically using commercial off-the-shelf (COTS) personal computer hardware and database software), commercial CMMS applications, or the newest approach; application service providers (essentially a web-based software rental service). This chapter reports on the current status of computerized maintenance management systems (CMMS) in use in hospitals and healthcare systems today and some of the future technologies that are starting to be used by the future-leaning providers of medical technology support services.

Computerized maintenance management systems can provide the technology management staff with a wealth of information to help manage many technology support-related functions. Examples include the following:

1. Quantitative equipment reliability assessments can be made based on failure rate, downtime and repair and maintenance costs. These assessments can be used to determine equipment that should be replaced, and assist in the subsequent vendor selection for the new product being purchased.

2. User/operator training needs can be identified based on trends in use error problems (e.g., problem not repeatable, "knobology", liquid spills, physical damage).

3. Scheduled maintenance can be prioritized based on the risk to the patient of an equipment failure and the maintenance needs of the device. CMMSs can be used to better balance and manage this often very large workload.

4. Scheduled maintenance program effectiveness can be measured by the rate of problems identified (yield), parts replaced, equipment not found/not available as compared to the total number of inspections performed by risk priority, and again, used to manage this often very large workload.

5. Workorder systems can be used to prioritize repair requests and better manage downtime of critical systems.

The remainder of this chapter is broken into the following sections: Medical Equipment Management Fundamentals, the CMMS Core, Other Key CMMS Modules, Data Integrity, Reports, Utilities, Network and Multi-user Issues, and "New" Technologies for CMMS.

Medical Equipment Management Fundamentals

Technology plays a key role in the delivery of today's healthcare. Keeping the medical devices that help provide that care in good working order is the role of equipment service management. In the year 2000, US hospitals spent over 3 billion dollars to service their medical equipment. Appropriate equipment service, whether performed by hospital personnel, equipment manufacturers or contracted 'third-party' organizations, is essential to modern, high-quality, cost-effective healthcare.

Modern healthcare organizations must carefully manage all equipment service independent of the service provider, who may be an employee, a contractor, a manufacturer representative or an employee of another organization affiliated with the healthcare institution (e.g., GPO (group purchasing organization)). Comprehensive equipment service management includes all medical technology and all service providers. In many cases there will be multiple service providers that may include multiple in-house groups (e.g., Clinical engineering, Radiological Engineering), multiple manufacturers, and multiple independent contractors. In other cases, there may be one in-house or contracted organization coordinating all the service regardless of who is the actual service provider for a specific device or repair.

In addition to the actual equipment maintenance and repair, the technology management team should be participating in all phases of a device's life-span including: capital budget planning, equipment needs analysis, specification and request for proposal/bid authoring, vendor selection, service provider evaluation and monitoring, service contract evaluation and monitoring, installation planning, installation, acceptance, user education, product recalls/alerts, incident and accident investigation, replacement analysis, de-installation and salvage. Overall program cost management is another key function.

Regardless of the service provider model, service is coordinated by a service manager who may be on-site in larger organizations, or may be shared among several sites for smaller hospitals. The service manager could be an employee of the healthcare organization, a contracted employee or an employee of a vendor. There are many different cost models for the payment of medical device service and it is the responsibility of the service manager to coordinate such service in an efficacious and cost effective manner within the defined description of the manager's job as directed by senior leadership.

Equipment Management Implementation

The first, and one of the most critical, steps in implementing an equipment management system (computerized or non-computerized) is to complete an accurate inventory of all equipment that will be under the equipment management program including devices that will be serviced by other organizations but whose service needs to be tracked. Each device that needs to be tracked must have an equipment control number assigned to it and labeled on the device. In some hospitals, the hospital asset number or property number already assigned to the device may be used as an equipment control number. If the asset tracking system is incomplete or the format of the asset number is not compatible with the equipment management system then an independent equipment control numbering system may need to be developed. Without an accurate inventory system it is impossible to accurately track maintenance and repairs, alerts and recalls and most of the other equipment management functions.

The inventory needs to be kept accurate and to be frequently updated as new equipment is added to the hospital's inventory and old equipment is removed. This involves policies and procedures that include the equipment management function as a critical part of the hospitals new equipment receiving function and equipment removal/salvage operations.

Important parameters to be tracked in association with each piece of equipment in the inventory are the model, serial number, warranty expiration date, risk of the device, type of device, ownership information, maintenance scheduling information, purchase information. A sample list of data fields and their definitions is included in reference 1.

JCAHO

The Joint Commission on Accreditation of Hospital Organizations has considerable impact on the equipment management program. The following is a discussion of some of the equipment management-related JCAHO requirements.

Standard EC.1.6: The hospital plans for managing medical equipment.

The intent statement for EC.1.6 starts as follows: >The hospital identifies how it will establish and maintain an equipment management program to promote the safe and effective use of equipment

The equipment management program is documented via the equipment management plan. This plan includes processes for the following: a). selecting and acquiring equipment; and b). establishing criteria for identifying, evaluating, and taking inventory of equipment to be included in the management program before the equipment is put into clinical use.

A hospital has the option of including all patient care equipment in its program or developing written assessment criteria and applying that criteria on a device-type by device-type basis to determine if a device is to be included in the equipment management program. All patient-care equipment must be assessed, independent of acquisition source, including rentals, leases, donations, and physician-owned equipment. The written assessment criteria should include the following:

- Equipment function (e.g., Does the device provide life support or a resuscitation function?),
- Physical and clinical risks to the patient: What is the likelihood that the device will fail in such a way as to cause serious physical injury? How is the device used or how is data from the device used? What would happen if the device displayed or reported clinical data erroneously?
- Maintenance requirements: Does the device require periodic parts replacement, lubrication, recalibration or other routine maintenance in order to perform properly and safely? What, and how frequent, is maintenance being performed by the user? What additional maintenance must be performed by the service provider?
- Incident history: Does the device have a history of incident reports or other serious reported problems?

Many different schemes have been developed to determine the risk associated with a given device or type of device. The simplest provide a three level categorization (high-risk, moderate-risk, and low-risk) for each device included in the equipment management program. Some systems also include the ability to define and identify critical systems. Also, dependent on local codes, standards and policies, low risk devices with no maintenance requirements may not need to be included in the plan.

In addition to the JCAHO, various other state, local, building code-related (e.g., NFPA) and professional organizations (e.g., CAP, ABBA) have accreditation requirements and licensing laws, regulations, and standards which vary by locale and type of institution.

Data Collection

The primary incoming data to the equipment management program are repair-information, scheduled maintenance workorders, new equipment receipts, product recalls and alerts, and incidents and other hazard information. This large amount of information needs to be collected in a user friendly, yet, controlled and organized manner. Non-automated means of collecting this data have been via paper forms for workorders (scheduled and unscheduled), telephone requests, and incoming equipment documents (internal documents or vendor packing slips).

Equipment data management schemes are typically based on each device's unique equipment control number as assigned by the healthcare institution or its contracted service management organization. A file is established for each device and associated repair and maintenance activities logged in that file. This file should include all maintenance and repair activities performed on the device regardless of the service provider.

With non-automated equipment management systems it is difficult to implement statistical analysis of the data including: cost center accounting information, device-type problem analysis and reporting and other statistical analysis for trending and reporting problems. When the inventory includes large numbers of devices, and therefore, large numbers of scheduled and unscheduled workorders, statistical analysis by non-computerized methods become overly cumbersome. Many large hospitals have more than 10,000 devices and complete more than 20,000 workorders in one year. Statistical analysis of this data must be performed in order to reveal useful trends of problems categorized by department, by equipment model and by type of equipment. These trends then become information that can be used to identify equipment requiring replacement, user training requirements by department, and user training requirements by type of device or model. Obviously, management of this large amount of data is one of the reasons that computers are used for modern equipment management programs.

Clinical engineers and hospital administrators are recognizing the cost and technical advantages of centralization in equipment management/maintenance services as can be seen by the increasing responsibilities that many clinical engineering departments and contractors are receiving. These include increased responsibilities in clinical equipment maintenance/repair (e.g., Radiology, clinical laboratory) and non-clinical equipment maintenance/repair (e.g., information technology equipment, telecommunications, material moving robots). In addition, as large hospitals purchase and/or jointly manage neighboring smaller hospitals, clinics, free-standing surgery centers and other healthcare-related facilities the repair and maintenance of medical equipment in those facilities is frequently coming under the responsibility of the parent organization's Clinical engineering department. As growth in responsibility, technical complexity and volume continues, it becomes clear that computerized data bases are required to handle the large amount of data and to convert that data into useful management information.

The Computerized Maintenance Management System Core

The core of an equipment management system is equipment inventory, repair and maintenance history and workorder control. The equipment inventory is an automated file of all the equipment that has been included in the CMMS. The repair and maintenance history is a record of each repair and maintenance event, independent of who initiated the event and who provided the service. Workorder control is used to dispatch and prioritize requested work, schedule periodic inspections and preventive maintenance, and track the status of pending scheduled and unscheduled workorders.

Equipment inventory

In the typical CMMS, when new equipment is received, a biomedical equipment technician (BMET) makes sure the order is complete, inspects and tests the device in accordance with the service manual provided as part of the order, and, based on the type of device, the organization's inclusion criteria and the policies of the clinical engineering organization, determines if the device needs to be included in the equipment management program. If it does the BMET then enters (or completes a form so a data entry clerk can enter) the new item onto the database as well as completing an incoming inspection workorder.

Device descriptions and other fields should be made as consistent as possible by using ECRI's standardized device nomenclature and relational database techniques (e.g., each unique model entry has one entry that is referenced by all equipment entries of that model). Each model and device type can also include various defaulted fields (e.g. scheduled maintenance information such as inspection frequency and maintenance procedure reference). A similar construct may be used for the owning department (cost center) with defaults for minimum scheduled maintenance frequency and location. This building block approach, with references to standard tables (e.g., departments, type descriptions) and built-in default values, allows equipment records to be built quickly with maximum data integrity and flexibility.

Reference 1 lists fields, and their definitions, that are typically stored as part of the equipment inventory.

For those new devices whose model and/or type description are not yet in the CMMS the equipment type record has to be built first, and then the model record before the new equipment record can be generated.

The integrated history record

The second part of the core of the CMMS is the integrated history record. Whereas, equipment records are fairly standardized across most CMMSs, the maintenance and repair records are not standardized nor is there a consensus on what data is necessary to collect. There is a large variation among CMMS regarding what data is collected, how the data is collected and how the data is used.

The integrated history record concept provides a service provider independent, date/time-tagged repair and maintenance history associated with each service event.

The fields for the integrated history record are listed in Reference 1.

The typical history record contains the following information:

1) Original problem/request: text of original problem request

2) Workorder type: category of work (i.e. scheduled maintenance, repair, incoming inspection, project, recall/alert)

3). Open date and time: Origination date and time

AND one or more tasks and each task contains the following information:

1) Start and end dates and times for times for each task.

2) Status of the workorder at the end of the task (i.e. complete, awaiting parts, referred to a vendor)

3) Service provider and tech/engineer identification: who performed the task (vendor or clinical engineering and which tech/engineer)

4) Labor hours for the task including travel, overtime breakout

5) Parts/materials cost for the task

6) Reference to a parts purchase order, vendor repair order or stock parts sales order associated with the task, as appropriate.

7) Downtime is another data field that is very important to track for high cost medical equipment (e.g., imaging equipment).

Associated with each task is a list of zero or more specific actions taken as part of the task. There is no consensus in the Clinical engineering community as to whether this additional important data should be encoded or free text. Certain special fields that cause other action(s) to occur must be encoded (e.g., codes that indicate the status of the workorder, codes used to update the scheduler due dates (e.g., electrical safety pass, inspection complete, PM complete). Other fields can be either free text or encoded. Free-text generally provides more comprehensible information; encoded data is easier to statistically analyze.

Workorder subsystem

The workorder subsystem of the typical CMMS consists of the following modules: an unscheduled (requested) workorder manager and technician dispatcher, and an inspection/preventive maintenance scheduler. Some systems also include a inspection/preventive maintenance procedure library.

The unscheduled workorder manager documents incoming requests for repair services and keeps track of the workorder until completion. Typical information tracked includes requestor name and phone number, equipment identification, equipment problem and/or service requested, equipment location, type of workorder (i.e. repair, new inspection, product recall/alert) and the priority of the workorder (i.e. how soon does the customer need the work completed). See Reference 1 for a list of fields and their definitions.

The maintenance scheduler is used to initiate and manage scheduled inspections, scheduled parts replacement and scheduled preventive maintenance workorders. Scheduled inspections are defined as periodic inspections that verify that the product meets manufacturer's specifications by using externally calibrated sources and measuring devices. Generally, scheduled inspections will be completed on-site and will not require removing equipment covers. Periodic parts replacements are replacements of specific pre-determined parts at predetermined intervals (e.g., replace ni-cad defibrillator batteries every two years).

Preventive maintenance(PM) are actions which are necessary or desirable in order to extend the operational intervals between failure, extend the life of the equipment and/or detect/correct problems which are not apparent to the user. Preventive maintenance may include scheduled parts replacement and inspection activities but PM is generally more invasive, typically requiring the equipment to be brought to a shop location and requiring access to the internal portions of the equipment. For example, lubricating the moving parts of an electric bed would be preventive maintenance.

In the typical CMMS, each item of equipment has associated with it scheduled inspection data that includes the following for each type of scheduled inspection: provider responsibility (i.e., what service provider is responsible for completing the inspection/PM), an interval (e.g., 12 months), fixed/floating flag, a synchronization date for fixed scheduling, the most recent completion date and the next due date.

The next due date is calculated based on either a fixed or floating basis. A fixed schedule results in the work being scheduled at the same time of year each year based on the interval and a synchronization date regardless of when the last inspection was completed. A floating schedule results in a new due date determined by the inspection interval and the date the last inspection was completed. Upon request, or at fixed times (e.g., once a week or once a month) the inspection scheduler initiates and prints, based on the parameters listed above, a summary or detailed workorders that are the scheduled work for the following period.

The inspection/preventive maintenance procedure library consists of a set of equipment type- and/or model-specific procedures itemizing the tasks and parts required to complete periodic inspections, preventive maintenance and periodic parts replacement. Some organizations use references to service manuals. Others develop typed procedures using word processors and reference those and still others use sophisticated CMMS-based procedures that use database fields for common tasks and build the procedures as sets of tasks. There is no consensus on the data format for procedures other than that model-specific procedures are required for most high-risk devices (e.g., ventilators) and complex systems (e.g, imaging systems).

It is required that technicians performing scheduled maintenance tasks consistently and appropriately test the device being inspected. Most CMMSs allow scheduled maintenance workorders to be generated as individual workorder forms with the itemized procedure on the printed workorder, or as a list of workorders with a reference to a printed procedure. Many commercial systems, provide both options and leave the decision to print procedures for each workorder to clinical engineering management.

Parts and Service Provider Management

One of the underlying philosophies of a quality CMMS is that all services be tracked and costs recorded regardless of the service provider. This sections describes various ways to track and manage repair parts and vendor services .

Parts

One of the ways to categorize repair parts is by the way that they are obtained. Repair parts are typically obtained from one of the following types of sources: 1). "stock" parts, 2). parts purchased directly from a vendor and shipped to the hospital for specific use on a specific repair or 3). parts supplied by the vendor as part of vendor service that includes installation labor.

Stock parts are parts that are stored locally for ***future*** use. These parts may be stored in a stock room, at a technician's workbench or in other locations. All clinical engineering departments maintain some stock of electronic components, batteries, wire, nuts, bolts and other common hardware. Many departments also stock circuit boards and other expensive medical-device specific parts.

The decision as to what parts to stock and what parts can be ordered on an as-needed (just-in-time) basis is based on how critical the device is and the ability of the Clinical engineering department to obtain specific parts from the parts source quickly. Since it is impossible to predetermine all failures and it is cost prohibitive to stock all parts for all devices, ideally, major high-cost, low failure rate parts would not be stocked.

Some clinical engineering departments have purchasing authority and issue their own purchase orders. Purchasing authority combined with a direct receiving function in clinical engineering and the availability of Federal Express, UPS or other overnight carriers allows the ordering and receipt of parts to frequently occur within 24 hours, therefore, minimizing the need to stock high-cost, low failure rate parts. However, some Clinical engineering departments are still burdened by institutional purchasing protocols that require the Purchasing department to pre-approve and/or place parts orders thereby adding significant delays to the ordering and receipt of parts. Computerized parts management systems are very non-standardized and typically differ a great deal from one department to another and one institution to another.

CMMS-based parts management software usually requires that all parts entered have a previously issued and unique clinical engineering part number. Alternatively, some systems do not require a unique clinical engineering-generated part number and just use the manufacturer's part number as the index to the parts management system. Other fields that typically are collected include a part description, price(s), manufacturer, manufacturer part number, vendor and vendor part number.

Most hospital purchasing and accounting systems are much more complex and require more complex systems to manage parts. For example, some clinical engineering departments stock large numbers of parts and/or high value parts and require that pricing include a handling markup to pay for parts stockroom overhead. Other departments may require pricing calculations based on a rolling average price paid when several parts (bought at different times and at different prices) are resold to the clinical engineering customer as part of a repair. Other institutions that rely on purchasing parts quickly on an as-needed basis may require a reference to a unique purchase order number or purchase order tag number for each purchase.

Service provider management

No clinical engineering department can provide 100% of the equipment service required 100% of the time on 100% of the equipment inventory. In order to control the cost and quality of vendor medical equipment repair and maintenance services, it is appropriate for Clinical engineering departments to control and coordinate vendor equipment services.

Vendor services can consist of non-billable warranty work, service performed on a fee-for-service basis, service performed under a prepaid service contract, billable services performed under a prepaid service contract but outside the prepaid terms and conditions of the contract, and other billable and non-billable services (e.g., product recalls, installation work). All costs (e.g., prepaid, billable, freight, tax, parts and labor) should be tracked.

All vendor service work needs to be coordinated and tracked in a similar manner to the data collected for in-house work. Typically, vendors complete service reports when they have completed a task, or leave the site even if the task has not been completed, and these service reports are one of the key documents used for data collection. Service reports should be required and provided to Clinical engineering for all vendor work, billable and non-billable.

In addition, billable services typically require a purchase order prior to the vendor providing the service. Billable services also will eventually yield an invoice itemizing pricing. Although estimated pricing for vendor services can be used to track costs, it is much better business practice for Clinical engineering departments to receive an invoice, match the invoice with the purchase order and service report, review the charges to make sure the cost is appropriate for the work that was completed and then complete the documentation by entering appropriate technical and cost data into the CMMS.

The CMMS requirements get more complex if maintenance insurance, partnership contracts and other risk-sharing, cost-sharing schemes (e.g., parts caps) are implemented. These typically require keeping track of various terms and conditions that trigger additional costs and/or rebates and sometime these triggers accumulate across a large number of pieces of equipment and/or multiple years.

Data Accuracy and Integrity

New equipment entries and equipment service history entries make up the majority of data collected in a CMMS. Service history data is typically collected by biomedical equipment technicians and then either directly keyboard-entered into the CMMS or a paper form filled out and data entry completed by a clerk. Equipment data can be entered by clerks or technicians from purchase orders and/or new equipment forms filled out by technicians for later entry by clerks. Service reports from other service providers are typed into the CMMS by technicians or clerks or scanned.

Data entry requirements are to optimize data accuracy while minimizing data entry times. Data entry times can be minimized by using defaults and not requiring any redundant entries or keystrokes. Data accuracy and data integrity can be optimized by making the CMMS easy to use correctly, enforcing data integrity rules when appropriate, and establishing operational policies and practices that make it every employee's responsibility to enter accurate and complete data.

Data integrity issues can be further subdivided as follows: data integrity enforced by the CMMS, data integrity enhanced (but not enforced) by the CMMS, and data integrity based on department-wide standardized definitions and operating procedures. Enforced data integrity can be used where flexibility in practice is not required and an absolute relationship always occurs. This occurs most often in customized CMMSs where the business rules can be built into the system and the flexibility of being able to match many different institutions rules are not required. An example of enforced data integrity would be that every parts purchase order must have a valid purchase order number, valid department and valid vendor associated with the order. In every case where there is an absolute requirement for a valid reference field it is appropriate to enforce data integrity!

Some fields require an entry but do not necessarily reference another table or file. Examples of these required fields are a model and manufacturer for each equipment control number, and start and end dates for each workorder. Other types of absolute data enforcement include the correct type of data (numeric, string, date etc), range checking (e.g., valid date checking), and inter-field relationship checking, sometimes called "sanity" checks (e.g., a workorder end date cannot be before the workorder start date).

When data integrity cannot be absolutely enforced by the CMMS because of exceptions or situations that require more flexibility than absolute data integrity allows, it is appropriate to use the same data integrity concepts but with defaults, warnings or workarounds that allow the user to 'legally' bypass the data integrity system. For example, when a new model is added, the CMMS may display a list of similar models and asks the data entry person to select one of the displayed models as the correct model nomenclature or indicate that the new model entered is indeed a valid new entry. This helps decrease the number of duplicate models inadvertently entered because of subtle differences in the model spelling and punctuation used, however, this does not preclude the entry of new model names.

Every department operating a CMMS should have a department-wide set of standardized definitions and operating procedures describing system use, data formats, data measurements, required fields and management's clarification of how they want certain tasks documented. For example, are transit time and wait time documented as part of a repair workorder? This set of standard operating procedures establishes a consistency that cannot be programmed into a CMMS (even a custom CMMS) and makes the CMMS a much more valid and useful management tool.

Reports

The reporting capabilities of a CMMS are the heart and soul of a vendor's product from a management perspective. The ability of the CMMS to produce relevant, informative, concise reports transform the software into a management

Table 1: Common CMMS Reporting Capabilities

Complete equipment inventory listing	Productivity Report by technician by date	List of vendor sources for repair parts by inventory number
Print scheduled PMs	Incomplete work orders by assigned technician, department and date	List of equipment manufacturers by equipment type, model etc
List of open, suspended, closed work orders by department, technician and date	Estimated PM hours by facility by date	Graph – bar chart Corrective repair costs vs. PM costs by date
Total work orders by facility by date	Life-Cycle-Costing by inventory number by date	Graph – bar chart Corrective repair costs vs. PM costs by date by inventory number
Total work orders completed by technician by date	FTE estimate based on estimated PM hours by facility by date	Personnel listing technician wage/salary, start date, certifications, OEM schools attended
PM completion percent by date	FTE estimate based on current corrective repairs By facility by date	Personnel listing vacation and sick hours available
PM completion percent by cost center by date	Total dollar amount for equipment in inventory	Risk Management SMDA reportable events by department by date
Total parts cost by inventory number by date	List of equipment by equipment type, category	Risk Management SMDA reportable events by date
Total corrective hours by inventory number by date	Weekly productivity by technician by date	Risk Management SMDA reportable events by inventory number by date
Incomplete PMs by technician by date	Graph – line chart of total inventory by date (from date-to date)	Risk Management SMDA reportable events by equipment category
Incomplete PMs total number by date	Graph – line chart of total inventory asset dollar value by date (from date-to date)	Graph Pie Chart of resources by PM hours and corrective hours by facility by date
Performance Indicator reports (e.g., downtime, response time)	Ratio of repair and maintenance cost to acquisition cost by type of equipment	Purchase order by vendor by date

tool. When justifying the purchase of a CMMS, a demonstration of reporting capabilities to senior administration is one key to whether or not the deal is consummated (with considerations for price). All successful technology management processes are dependent on the ability to gather data, aggregate the data to convert it to useful management information, and then produce reliable decisions based on the information. Reporting is the fundamental communication and decision support tool for the CMMS.

The ability to make the CMMS work towards your specific needs centers around the reporting capabilities of the system. The reporting access structure should be easy to use and intuitive, yet offer sufficient reporting power to allow any data field to be aggregated and reported in any manner that the end-user feels is appropriate. Typically, a tiered approach is used with "canned" reports for commonly used reporting requirements (e.g., monthly reports to customers), ad-hoc reports for selection of various fields commonly reported (e.g., equipment history reports with date ranges) and custom reports for more complex reporting requirements (e.g., cost benchmarking) that may require some programming skill to generate.

Point-and-click structures should be the reporting baseline with common graphics or symbols which are easily recognizable and understood regardless of the computer literacy of the staff. Microsoft Windows®-based structures are one way to provide familiarity and user-friendliness. More advanced reporting tools may also use a structured query language (e.g., SQL) to extract data from the database and additional (often third party) reporting tools (e.g., Crystal Reports®) to format and write the report. The CMMS must have a reliable query process that allows an interface with the main database for all required reports. Reports should have the capability to not only write to paper but also to view on screen and to "publish" them as computer transmittable files (e.g., PDF files), and/or web pages (e.g., HTML files).

All CMMS products will have generic reports. A review of the vendor's generic reports may reveal a need for reports specific to your healthcare facility. Specific reports can be generated utilizing *user-defined fields* or through custom reports written by the vendor, a third party, internally by information technology (I.T.) or clinical engineering department staff depending on resources available and the report writing tools available in the CMMS. The authors recommend that you include an agreement with the original vendor into the contract price for all initially required custom reports. Third party software vendors may charge as much as $50,000 per customized report.

Pop-up displays that are triggered by *indictor* limits provide a "dashboard" for decision support and management control (see chapter X *Using Medical Technology Assessment as a Tool for Strategic Planning* for an explanation of indicators and indicator flow charts).

The CMMS must be capable of satisfying regulatory reporting requirements, particularly those of the Joint Commission for the Accreditation of Healthcare Organizations (JCAHO), Food and Drug Administration (FDA) and local and state health agencies. The basic reporting structure for clinical engineering should include; an inventory list for all medical equipment, a work order generation and completion process, risk ranking of medical devices, preventive maintenance scheduling, personnel time allocation, and resource allocation (both physical and personnel). Table 1 is a list of common reports.

Utilities

A utility is a computer program not contained in the main operating system (OS) or the core CMMS that provides an essential function or feature. In most cases, as customers demand similar utilities they are incorporated into the OS and/or CMMS, but during selection of the CMMS for your facility it is wise to have a checklist of features required.

Features, which are required but not contained in the OS or core CMMS, should be available from the vendor as a utility. Examples of utilities are database validation, database diagnostics, security features, global data changes (e.g., manufacturer A merges with manufacturer B), user defined fields, initial installation, setup, database conversion from a previous vintage or "foreign" vendor's CMMS, and configuration programs.

The system administrator has access to the utilities programs and will become familiar with their functions. General CMMS users will most likely not be aware of or have access to utilities programs. As the needs of your facility change, available utilities programs allow your CMMS to become flexible and scalable. The addition of a utilities program allows your system to grow as your needs change without the expense of replacing the entire system. This is an important purchase consideration and should be explored thoroughly.

Network and Multi-User Issues

All but the very smallest of clinical engineering departments will require more than one user with simultaneous access to the CMMS. The connectivity and throughput capabilities of your CMMS will be determined by the existing network, or the funding available to purchase and install the recommended network infrastructure. Prospective CMMS vendors should provide you with network bandwidth requirements for their system. Ask the vendor for complete technical specifications and review those specifications with your IT department

The optimal CMMS vendor selection process should involve a committee, which includes a staff member from the IT department. Begin with a list of your multi-user needs and expectations. Is there a need for telecommuter system access? Do you have a single facility or multiple local or remote facilities with varying telecommunications capabilities? Who are your customers? Who are the system users? How many *workstations* will be required? After answering these questions, compare your needs to the system capabilities and the institution's current network infrastructure. Can you accomplish what you desire within the existing infrastructure? If not, what will it cost to provide a network capable of meeting your needs? Will funding be available to upgrade the network?

Assuming that the funding and/or the network is suitable for the needs of the organization, review the available networking technology. Are there areas where a wireless interface is more cost effective or will the entire network be hard-wired? Will you run the system on an intranet corporate enterprise network, an Internet Web-based network, a local area network (LAN) or a combination of these technologies?

Most CMMS will use a client/server, local area network (LAN) structure for multi-user access. The client/server system consists of a main server (or multiple servers if the CMMS is operating across multiple facilities) and several workstations typically interconnected via a cabled network. The typical workstation will be the personal computers (PCs) in your work areas and will be used to run the CMMS client and other desktop-based applications (e.g., word processor, spreadsheet, calendar). The server is a more robust computer with the power and memory to host and drive the entire system. All CMMS data will be stored on the server and sent to the client workstations on an as-needed basis. The server may be located in the clinical engineering or information technology departments and is managed by the system administrator.

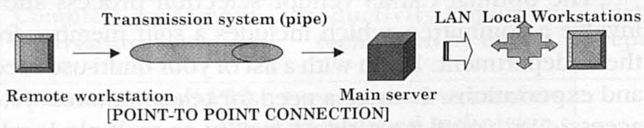
For those mobile users who cannot often access a LAN-connected workstation, most CMMS vendors offer a laptop, standalone version that can be periodically, intermittently connected to and resynchronized with the server.

Data Telecommunications Technology Primer

Most hospitals will have existing network infrastructure (cabling, routers, switches, hubs etc). If applications are required for remote workstation interfaces (those outside the LAN framework), an understanding of the available Local Exchange Carrier (LEC — local telephone companies or competing companies that can provide you with the desired connectivity) telecommunications infrastructure is essential.

For connectivity over longer distances than the internal wired LAN/WAN, there are a variety of telecommunica-

Figure 1: *Point to Point Remote Communications*



tion options including; microwave, optical and various wired technologies. Microwave connections can only be considered for short (line-of-sight) distances of less than 3 miles. Rain, snow, fog and birds can cause network interruptions of microwave transmissions. Infrared transmission, known as Free-Space Infrared Local Area Network (FIRLAN), may also be used for remote connection to the LAN. FIRLAN advantages and disadvantages are similar to those of microwave and installation costs can run above $20,000. These types of remote interconnections to the LAN are known as point-to-point connections. Figure 1 illustrates a generic point-to-point telecommunications system.

The rate of uninterrupted flow of information is known as throughput. Throughput is directly related to available bandwidth and router capacity. Table 2 illustrates the various LEC services and their bandwidth limitations.

Table 2: *Comparison of Communication Network Technology*

SERVICE	CARRIER/ MEDIUM	BANDWIDTH	DATA INTEGRITY	APPLICATION (S)
PSTN (standard phone cable network)	4-wire dedicated	56Kbps	Moderate to very good	Remote PC/workstation to LAN PC
Full T-1 24 digital channels	T-1	64 Kbps/ channel	Excellent	Supports video capabilities. Only fractional T-1 required for most CMMS applications
Switched 56	Fractional T-1	56 Kbps	Moderate to very good	Remote PC/workstation to LAN
BRI	ISDN (2 B + D)	128 Kbps	Excellent	Must have an ISDN interface for legacy equipment
Frame Relay	ISDN 2-wire	64-128 Kbps	Excellent	Also supports wireless applications
Broadband	Optical fiber & ATM	>1.5 Mbps	Excellent	Supports video applications. Not required for general CMMS applications

The primary network issues involving the installation of your CMMS will involve your local area network (LAN) and access to a server. A network consists of nodes (workstations, hubs, media access unit (MAU), bridges, routers and gateways), that are linked together for the purpose of transmitting data from one location to another location. LANs provide a robust, flexible, and scalable means to interconnect all users of the CMMS. Although LAN standards are beyond the scope of this book, further in-depth information concerning LAN specifications can be found in the Institute of Electrical and Electronics Engineering (IEEE) 802 family of standards.

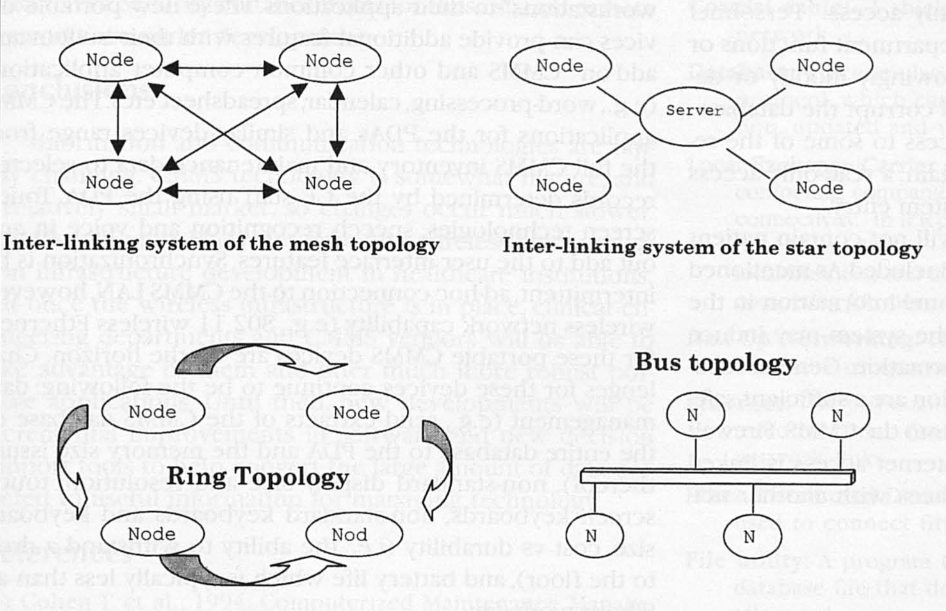
LANs are constructed in specific layouts (connection pathways) known as a topology. The major LAN topologies are mesh, star, ring and bus. Figure 2 illustrates each of these topologies, which provides a visual concept of how various networks are linked together.

The bus and ring topologies are the most common LANs. Star and mesh topologies are more expensive due to the increased number of links in the network. Bus and ring topologies are both well-suited for CMMS applications. Bus topology with standard Ethernet (10Mb/sec) or high-speed Ethernet (100Mb/sec) are the most commonly used LAN infrastructure for CMMS applications.

The principle of ring topology involves a *token*, which contains requested information and is passed around the ring until it is accepted by the originator of the request (workstation). Ring topology assures uniform distribution of requested information and guards against bandwidth saturation. Both shielded and unshielded twisted pair can be used at transmission rates up to 16 Mbps, which is a little higher than standard Ethernet bandwidth. Bus topology has an advantage of simplicity for maintenance but access depends on the position of the workstation on the bus.

Each LAN will have one access method and one or more specified physical media and topologies. The most typical LAN uses bus topology and Ethernet. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD) as the access method. Ethernet refers to the physical link and data link protocol for LAN interconnection. The physical connection may be a twisted pair or coaxial cable. The maximum transmission rate of an Ethernet link is 14,800 - 64 byte packets per second (PPS) or more commonly 10 Mbps.

Figure 2: *Mesh, Star, Ring and Bus Toplogy*



Ethernet connections which use twisted pair phone wires will have an RJ 45 connection at the terminal end and are known as 10base-T. High-speed Ethernet, which has a transmission speed of 100 Mbps, is known as 100base-T.

If the facility has sufficient network infrastructure to meet the bandwidth requirements of the CMMS, then the clinical engineering department should use that infrastructure. Table 3 provides a comparison of physical media and LAN topology characteristics.

In some instances, it may be cost effective for the facility to purchase one CMMS, which can be utilized by multiple service departments such as IT, physical plant and clinical engineering. Difficulties arise in this scenario due to multiple departmental regulatory reporting requirements and variations in project priorities. If a single server is used the drive should be segmented by department. This allows easy access to information pertaining to your department. Without segmentation, all data is lumped into one large pool. The queuing factors must sort through several lists before the specific information you require is retrieved.

Although it is more expensive, a dedicated server for each department eliminates several software conflicts, is simpler to install, customize, upgrade and maintain, and reduces problems with throughput.

Additional challenges of a multi-user network involve access levels and access security. The system administrator is required to have access to all features and functions and manage security and access for the other staff. The manager and supervisors, administrative assistant/clerical/dispatch, and technician staff may all have access to some common features and some other features dependent on their access group. If a nurse manager is concerned about a shortage of vital signs monitors, a read-only access level provides information on the repair status for a specific piece of equipment. Allowing clinical staff "read-only" access to CMMS inventory and work order status screens is an efficient communications and management tool. End-user access to enter new repair workorder requests may also be useful.

The system administrator will have the highest access level capable of performing all CMMS functions. A supervisor access level just below the system administrator should be available for managers. This level of access provides reporting capabilities and sensitive personnel information concerning salary, date of hire, home telephone number and other personal information.

Table 3: Physical Media vs LAN Topology Comparison

Topology	Bus, star or ring	Bus or ring	Bus or ring	Bus, star or ring
Physical medium	Twisted pair	Baseband coaxial cable	Baseband coaxial cable	Fiber
Maximum nodes	About 250	About 1000	3,000-4,000	3,000-4,000
Available channels	Single channel	Single channel	Multi-channel	Multi-channel
Maximum transmission rate	100 Mbps	100 Mbps	400 Mbps	Several Gbps
Disadvantages	Lesser bandwidth, susceptible to noise	Susceptible to noise	Expensive, requires headend set up	Expensive, specialized training
Advantages	Low cost	Ease of installation	Transmission of voice, data, and video	Transmission of voice, data and video

General access should be available to all technicians and engineers in the CE department. Personnel outside the department should be given read-only access. Personnel without a knowledge of how your department functions or how the CMMS operates may unknowingly modify or delete important data fields or files and corrupt the database. Senior administration may desire access to some of the reporting capabilities of the system. Again, a read-only access level is the prudent approach for system entry.

Although most CMMS systems will not contain patient information, system security must be included. As mentioned earlier, there may be sensitive personnel information in the database and users unfamiliar with the system may induce errors requiring hand reentry of information. General security methods using password protection are a sufficient safeguard to prevent unauthorized entry into the CMMS. Firewall protection must be considered if Internet access is linked to the system or if the CMMS interfaces with another network.

New Technologies

Innovations and new applications of existing telecommunications and computing technology are emerging at a rapid pace. To state that you are implementing *new technology* is relevant only when describing the comparison to your facilities existing technology and in a specific, and short, time reference. The Internet and Computer-Telephony Integration (CTI) are perpetual cutting edge concepts that continually infuse new technology into the mainstream of networking. Add to this warp speed of transformation the nanotechnology of electronics and the entire world of networking takes on new meaning almost daily.

The most dramatic impact in telecommunications has come from and will continue from deregulation ushered in by the Telecommunications Act of 1996 and the resulting impetus for development of additional infrastructure. Satellite communication, fiber optics, ISDN, DSL and a host of other faster broadband communication technologies are bringing more and more data to homes and businesses at a faster and faster rate. Internet Web-based programs offer flexibility and accessibility unparalleled by any existing hard-wired LAN system. Virtual Private Networks (VPNs) offer the opportunity to have LAN types of applications on a world-wide scale. The availability of wireless network links (e.g., 802.11 Ethernet, Bluetooth) will undoubtedly be included in the networks of the future. Remote and distributed, computing technologies will overcome problems with scalability, performance and cost, the bane of hard-wired networks.

Technologies which are currently available (2001), but not widely utilized in CMMSs include: Personal Digital Assistants (PDAs), CMMS-like software imbedded in test and analysis equipment, bar coding interfaces, remote diagnostics, service manuals and operator manuals residing on a server or Web site, e-mail interfaces, video, technical and clinical in-services, and Web-based CMMS programs.

Several CMMS vendors have interfaced Personal Digital Assistants (PDAs) and similar handheld or "wearable workstations" to their applications. These new portable devices can provide additional features with their built-in and add-on CMMS and other common computer applications (e.g., word-processing, calendar, spreadsheet etc). The CMMS applications for the PDAs and similar devices range from the full CMMS inventory and maintenance data to selected records determined by the CE staff using the PDA. Touch screen technologies, speech recognition and voice in and out add to the user interface features. Synchronization is by intermittent, ad-hoc connection to the CMMS LAN, however, wireless network capability (e.g., 802.11 wireless Ethernet) for these portable CMMS devices are on the horizon. Challenges for these devices continue to be the following: data management (e.g., send extracts of the CMMS database or the entire database to the PDA and the memory size issues thereof), non-standard display size and resolution, touch screen keyboards, non-standard keyboards and keyboard size, cost vs durability (i.e., the ability to withstand a drop to the floor), and battery life which is typically less than an 8 hour work day.

Several CMMS vendors have interfaced preventive maintenance (PM) software into test and analysis equipment for paperless maintenance inspections, work orders, and electrical safety testing. Historically, these systems have focused on electrical safety testing and storing electrical safety leakage current values which has very limited, if any, legal or practical application. Automated integration of test equipment with a CMMS application may have some application where there are large numbers of devices that can be automatically tested and certain limited, critical data values stored.

Bar coding has been used by CMMSs for many years. Bar-code systems and readers have improved to where they are useful for equipment and parts inventory control and may have some utility in workorder management.

Various paging systems have been interfaced to CMMSs to allow automatic paging based on user entry of workorders and directed paging based on staff availability schedules and other data. As cellular phones, pagers, PDAs and other devices all get integrated, there is an opportunity to develop a "technician communication tool" that combines several of the features discussed here as individual products. To be most useful such a product would need to have seamless wireless network access to the full CMMS (e.g., IEEE 802.11 wireless Ethernet).

Another new technology is application service providers (ASP). ASPs are software applications running remotely at a vendor's site that are accessed by the end-user in a similar fashion to the way applications are accessed by LAN. A CMMS ASP would look little different than a LAN CMMS with a web browser as the GUI (graphical user interface) to the CMMS. The vendor of the ASP takes care of all the access and security issues as well as backups, upgrades and regular data maintenance. Fee structures are under development and include fees based on the amount of data stored, the number of users, bandwidth requirements and other parameters. Security enhancements for these shared remote networks are under development.

Conclusions

Information and communication technologies are rapidly changing. CMMS technology is somewhat mature, and a relatively small market, so changes occur much slower. CMMSs will most likely not drive the wireless communication infrastructure development in healthcare institutions, but once the wireless infrastructure is in place, clinical engineering departments and CMMS vendors will be able to take advantage of them and offer much more robust portable applications. Until then, new developments will be incremental improvements in software and new decision support tools to help convert the large amount of data collected to useful information for managing technology.

References

(1) Cohen T. et al., 1994. Computerized Maintenance Management Systems for Clinical Engineering, an AAMI Management Information Report, AAMI.

(2) Conrad, James W. ed. (1998), Handbook of Communications Systems Management, CRC Press, Auerback Publications, New York.

(3) Cram, Nicholas (1998), Computerized Maintenance Management Systems: A Review of Available Products, Journal of Clinical Engineering, 23:3 pp 169-179.

(4) Held, Gilbert (1999), Handbook of Communications Systems, John Wiley & Sons, New York.

(5) Held, Gilbert (1996), Ethernet Networks 2nd ed., John Wiley & Sons, New York.

(6) Held, Gilbert (1995), Practical Data Communications, John Wiley & Sons, New York.

(7) Sloan, John P. ed. (1997), Handbook of Local Area Networks, Auerbach, RIA Group, Boston.

(8) Barta, Rebecca A., 2001. A Computerized Maintenance Management System's Requirements for Standard Operating Procedures, Biomedical Instrumentation and Technology, Vol 35, number 1.

(9) ECRI, 1994. Inspection and Preventive Maintenance System.

(10) JCAHO, 2000. Comprehensive Accreditation Manual for Hospitals.

(11) Stiefel, Robert ed, 2001. Medical Equipment Management Manual, How to be in Complete and Continual Compliance with JCAHO Standards, AAMI.

Appendix A: Glossary of Additional Terms included in this chapter

Asynchronous Transfer Mode: A high speed network, which provides optimal multimedia transmission at prohibitive costs.

Basic Input/Output System (BIOS): Instructions stored on the motherboard for the purpose of coordinating the operation of system hardware.

Bridge: An electronic device that interconnects two disparate LANs.

Bus Network: A network topology where all workstations are attached to the same main physical medium (wire or cable).

Coaxial cable: A shielded cable for linking nodes within the network.

Database: A accumulation of information stored in an orderly protocol, which can be accessed through a query application, updated and viewed.

Local Exchange Carrier (LEC): The local telephone companies or competing companies that can provide you with the desired connectivity. In telephony jargon they are divided into Incumbent LECs (ILECS — the company who has a majority of the local business) and competitive LECs (CLECs – the company(s) competing for more of the ILECs business.

Dial Up Networking: The ability to enter a network from a remote site using a telephone or cable modem.

Ethernet: The physical link and data link protocol for LAN interconnection. One of the oldest and most cost-effective network links.

Fiber Distributed Data Interchange (FDDI): The physical link used to connect fiber networks.

File utility: A program that manipulates information from the database file that defines where files are found, sized and allocated.

File Transfer Protocol (FTP): A technique or process that allows transfer of files from one computer to another computer over the Internet.

Graphical User Interface (GUI): A graphical tool that provides the user with point-and-click, intuitive characters or icons to control the actions of the computer.

Hypertext Transfer Protocol (HTTP): A computer standard, which allows computers operating in different environments to transfer data.

Hub: A network node, which serves as a multiport repeater to other links in the network.

Intranet: A private network utilizing Internet-based technologies within an organization or enterprise.

Local Area Network: A group of computers sharing a common database and or server for a common purpose(s) forming nodes connected by a physical medium.

LOL: Internet chat-talk for laugh-out-loud.

Network: A system of nodes (workstations, hubs, routers, bridges, and gateways) which are linked together for the purpose of transmitting information (voice, data and video) from one location to another location.

Multimedia: A transmission which contains test, sound, video and graphics all of which are capable of being displayed by the user.

Server: A more robust computer with the horsepower to drive the entire system.

Throughput: The rate of uninterrupted flow of information.

Topology: The construction or physical geometric pattern of specific layouts (connection pathways) for a LAN.

User-defined field: An open field, which allows the user of a CMMS program to determine the characteristics of the queuing requirements and display outputs.

Utility: A small computer program not contained in the operating system (OS) that provides an essential function or feature.