Data Management of Telecommunications Power Systems
The Case for an Open Standard

Frank Bodi
Silcar Telepower
Level 1, 173 Burke Road Glen Iris
Victoria Australia 3146
frank.bodi@silcar.com.au

Paul Davis
Rectifier Technologies Pacific
18 Joseph Street Blackburn North
Victoria Australia 3130
pauldavis@rtp.com.au

***Abstract* – Currently, there is no global, open data or network management standard in the telecommunications power sector. There is a growing awareness that this represents a significant cost to telcos and asset managers. This cost may be measured both in capital, deployment and operating costs as well as indirect future costs. The cost-effective management of real time monitoring and asset information is a universal problem impacting all telcos.**

The paper will outline the kinds of information flow in telepower energy systems and how an open standard could provide cost savings and encourage wider adoption. It discusses what should be standardized and the process by which this might be achieved. The paper discusses common open protocols and data standards (e.g. SNMP, XML) and their application to a telepower standard.

An outline of current initiatives towards an open standard is presented. The paper presents a case for an open standard in the area of information (data) management, remote (protocol) monitoring and configuration of telepower systems.

This paper has been prepared collaboratively between Frank Bodi of Silcar and Paul Davis of Rectifier Technologies Pacific, out of a common technical interest. The Companies do not have commercial dealings with each other in this or other fields of business.

I. INTRODUCTION

A general trend in telecommunications has been to move towards centralized management of networks into the telco's Operations Support System (OSS) environment and this has included telepower. This central location is often known as a Network Operation Center (NOC). The main motivations are operational cost savings and increased quality of service by centrally locating technical specialists. This centralization makes it more economical to invest in sophisticated Network Management Systems (NMS). The deployment of NMS provide NOC operators with a uniform view of all parts of the network.

At the most basic level the NMS is used for monitoring equipment alarms throughout the network. In telepower systems this has meant the monitoring of alarm contact closures. This requires specific interfaces to be built to channel contact closure information from multi-vendor equipment into a homogeneous format the NMS can readily accept. The interfaces include both physical protocol adaptors and software interface modules. The development costs of such interfaces must be borne by the telco.

Telcos have realized the potential to do more advanced remote monitoring and configuration of equipment in the network. Beyond alarms, system critical parameters allow NOC operators to make more informed decisions on how to respond to a call-out. This can reduce operational costs. For example, service personnel may not need to be rushed to an isolated site. The potential to remotely configure systems, carry out remote routines including battery discharge, full alarm testing and site auto-discovery are features that would dramatically impact operational costs and network reliability.

As Computerized Maintenance Management Systems (CMMS) increase in sophistication, the ability to leverage standardized interfaces is not restricted to real-time monitoring of physical telepower equipment. The movement of data in and out of the CMMS is an important issue affecting data quality and bottom-line operating costs. Examples include general asset management, on and off-line access by mobile field personnel, business to business data exchange and the movement of data between industry applications. Advances in readily available open standards and protocols have made these considerations a practical reality.

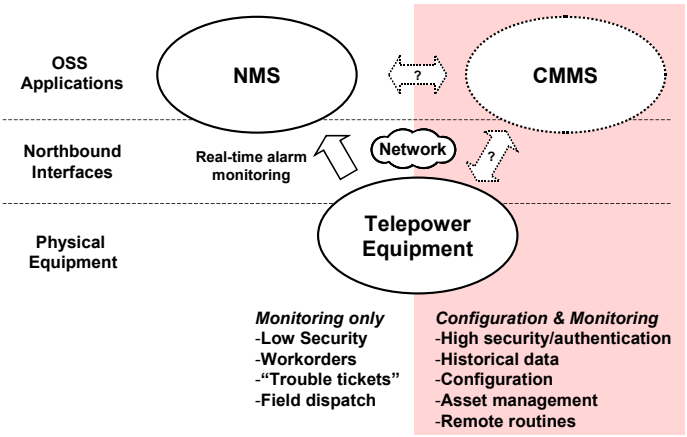
A survey of major telepower vendors has shown there is currently no cross-vendor standardization in remote monitoring systems. Open interfaces and protocols enable cheap, wide-spread information sharing in telepower systems. A standard is needed to define both the data to be found in telepower equipment and the protocol used to access this data. Protocols and standards such as SNMP and XML have emerged as popular IP based platforms of choice. In the last 10 years, significant globalisation has occurred in the telepower industry. Consequently a *global*, open telepower standard is needed to address what is widely regarded as the single most inhibiting factor in the large-scale uptake of intelligent network management of telepower systems - *cost*.

II. INFORMATION FLOW IN TELEPOWER SYSTEMS

It is difficult to generalize on the kind of network management systems most telcos are operating. The range includes systems with minimal alarm monitoring, legacy alarm-only systems and more advanced networks having access to analogue parameters, remote configuration and control.

In a telco data switch network, the information flow from the switching equipment (network elements) to management systems is often termed the "Northbound Interface". Information flow in a telepower network Northbound Interface may be broadly broken into two key areas. The unshaded portion of Figure 1 depicts real-time alarm monitoring applications, generally requiring a low-level of security. This is where the core volume of information flows - from physical telepower equipment to the NMS. This may also include on-demand access to low-level monitoring information by NOC operators and field personnel.

Figure 1 – Sources of Information Flow



The shaded portion of Figure 1 depicts interaction with CMMS which are used to facilitate operational workflow and asset management. To a lesser extent, these systems may interact with the real-time NMS in the creation and scheduling of work orders, the storage and capture of performance and historical operational information such as alarm history and faults. Probably to an even lesser extent, the CMMS system may be used to remotely access, configure and control asset information embedded in telepower plant. Such activity may require a higher-level of security such as authentication and encryption.

It can be expected that the demand for high-quality information will continue to grow rapidly in the future. Such demands will place increasing pressures on key infrastructure to provide access to information that is not currently available. New information paths will be created in the delivery of improved services and the search for new revenue streams. These demands could see wider information access to telepower equipment infrastructure and CMMS systems by equipment vendors, telco customers and expert contractor staff.

Existing volumes and types of information flow will not remain static. Standardization of information storage and protocols are needed to satisfy the increasing demand for information flow.

III. CASE FOR A GLOBAL TELEPOWER STANDARD

The key benefits of an open telepower data standard are both a core business and IT goal - reduced cost of OSS network management infrastructure & increased visibility of network assets. For network or Internet related products and protocols, highly proprietary solutions seldom find a commercial niche. In the IT industry the benefits and future-proofing of open standards and protocols are accepted as a matter of course. These include reduced cost, better security, greater flexibility and increased interoperability between software applications and systems. So strongly are these values entrenched, that in recent years even Microsoft™ has been forced to embrace technologies based on open standards and protocols. It is considered that the same arguments apply to the protocols and standards used in network management of telepower systems.

There are a number of key reasons why a global, open telepower data standard is needed:

- Keep downward pressure on the capital cost of emerging, intelligent network and alarm management system hardware and software.
- Keep downward pressure on future cost spirals generated by highly proprietary solutions.
- "Future-proof" the technology as far as practical, by using proven protocols and standards that are more likely to have widespread support in the foreseeable future. No technology can ever be made completely future-proof, nevertheless the choice of standards based on simple, proven and popular technologies such as SNMP and XML certainly prolong product life-cycle. When a technology reaches end of life-cycle, a main-stream technology has more support in transitioning to a new technology, than one which is isolated and proprietary.
- Remove high vendor dependencies in an area that is particularly sensitive to all telcos. The network management system is the "heartbeat" of asset management and service delivery. Telcos may be reluctant to commit to proprietary designs that effectively create a high dependency on single vendors.
- Help maintain a single network management interface in multi-vendor environments. Building a single interface to a multi-vendor network is not technically difficult; there are however, many hidden costs associated with protocol conversions including licensing of protocols, updating the conversions each time a vendor implements

changes, keeping track of change management in a multi-protocol environment. These issues all add cost which can remain largely hidden when a decision is made to commit to a technology.

- Reduced risk of networking, data and interoperability flaws. These may arise from competing vendor systems that do not inter-operate very well, leaving occasion for errors in remote configuration and control.
- Open protocols and standards are more secure, having been extensively tested through widespread usage, and are more likely to remain up to date than closed protocols.
- Greater ease introducing advanced technologies such as auto-discovery. Auto-discovery technology relies on standardized protocols that enable new sites to be learned. Such features are much harder to realize in multi-protocol systems. Auto-discovery reduces operating cost through automatic notification and asset mining of new sites. The risk of omitting sites as they come on line is reduced increasing system reliability. All telepower systems rely on continuous monitoring to maintain high network reliability. In any large telecommunications system, there will be incidences of hidden assets that either dropped off or never made it to the "monitoring radar", impacting both cost and reliability.
- A homogenous view of asset information and integrity, regardless of who the vendor is. Uniformity is needed to reduce the effort of asset management and provide a clearer view of asset information.
- Standardization, particularly in network systems, leads to the ready availability of key networking components. One example is the element manager module required for interfacing with legacy dry alarm contacts. There are many commercial products available that provide this facility i.e. conversion of analogue and digital signals to a communications protocol. In the absence of an open standard, these products cannot readily afford a uniform view. Even those that conform to an open protocol such as SNMP, still do not have a standardized SNMP Management Information Base (MIB). In Australia there are some 30,000 systems operating from alarm terminal strips. Globally the number is conservatively estimated to be many million. The current situation is that every vendor develops their own software to embed in these modules. Development costs are amortized on a relatively small number of units – resulting in higher prices to telcos.

Network Migration Strategies

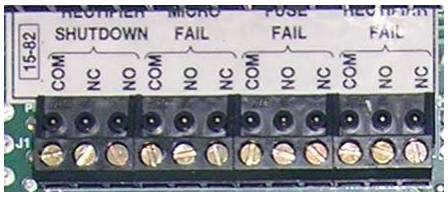
The following discussion considers how an open standard may impact the migration from a network with basic alarm only monitoring to one with intelligent monitoring. It is assumed the existing network consists mainly of legacy equipment (alarm contacts) and a proportion of newer equipment with intelligent remote monitoring. It is acknowledged this scenario will not apply universally, some telcos having already adopted proprietary intelligent monitoring systems, others having more basic networking.

"Typical" Telepower System

Today the alarm contact terminal block remains one of the most common-place interfaces to telepower and other equipment. The terminal block has been used universally for many years and has a number of attractive features including:

- Simple for vendors to implement, low-cost.
- Set points and features may change internally for different applications or markets but the alarm contact strip stays the same – a wire termination.
- Every power system has one, thus the "de-facto standard" status.
- Represents both a physical and logical interface.

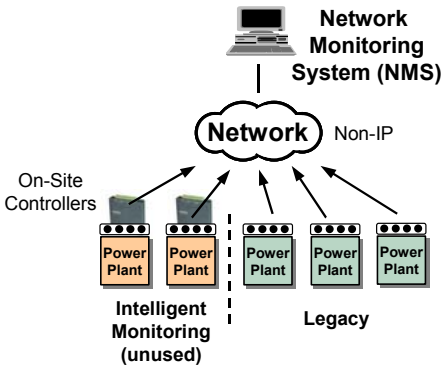
Figure 1 – Alarm Terminal Strip, "De-facto Standard"



In effect, the alarm terminal strip has helped bring some uniformity to legacy alarm monitoring in multi-vendor systems.

As telcos request greater intelligence from their systems, power systems are now routinely supplied with intelligent monitoring accessible over an IP network. Many telcos are in the situation depicted in Figure 2, with a large portion of legacy systems, and some newer equipment with intelligent monitoring.

Figure 2 - Legacy Power Plant Alarm Contacts, RS 232, 422, etc

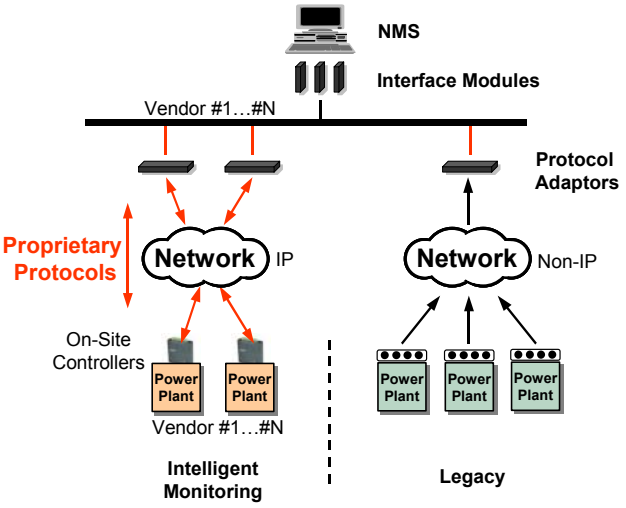


Migration - No Open Standard

To introduce intelligent monitoring network-wide, there are broadly two kinds of power equipment to be considered. Those that already have on board intelligent monitoring, and those that do not. The latter will probably form the bulk of systems. If the centralized NMS is to remain homogeneous,

protocol adapters are needed to reconcile older legacy systems and newer multi-protocol intelligent systems. These adapters could be located centrally, or some vendors have products that co-locate with the power plant, converting local RS232/422/485 signals into their preferred network IP protocol. Either way, protocol adapters are needed both for old and new power systems. Since there is no open standard, the conversion of all these proprietary protocols will likewise be to a chosen proprietary protocol. The NMS will also require customized software interface modules to provide an interface with the physical protocol adapters.

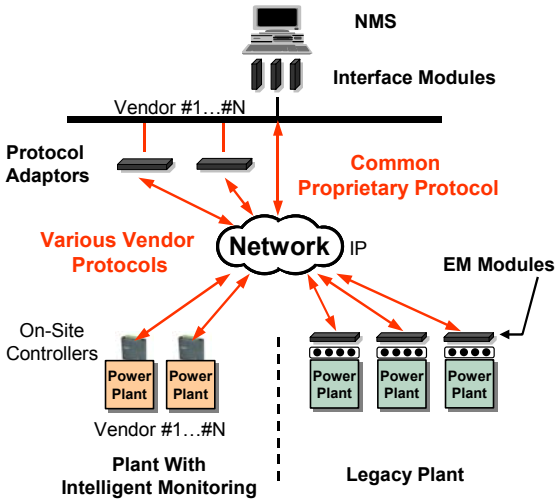
Figure 3 – "Typical" Telepower Systems



The legacy systems shown in Figure 3 have been adapted to the new network, but since they only provide signals from an alarm terminal strip, cannot offer intelligent services. To complete the conversion, an intelligent element manager (EM) module is needed that will accept signals from an alarm terminal strip, as well as other analogue parameters and provide any intelligent functions that are deemed necessary. A network with EM modules is depicted in Figure 4. A software interface module is still required to interface these modules to the NMS.

As can be seen, the resultant network has potentially many protocols.

Figure 4 – Intelligent Monitoring, no Open Standard



In the network of Figure 4:

Number of Protocols = k x Number Vendors
Where k >= 1

In other words, the total number of protocols is in general equal to or greater than the number of vendors, assuming the common protocol belongs to one of the existing vendors.

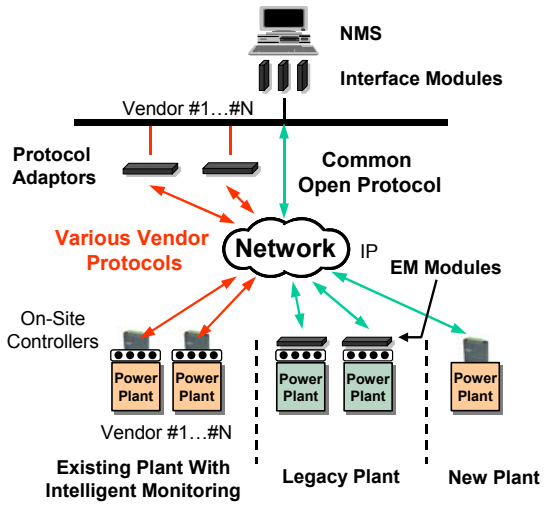
This situation is undesirable for a number of reasons:

- As mentioned previously, the potential world market for EM modules is considerably larger than is present in any single telco business sector. Total expenditure on development effort will be considerably larger if this effort must be repeated for every different market. Even globalization of telepower vendors will not necessarily help if each telco community selects a different common protocol.
- Multiple protocols will incur significant cost overheads that become increasingly difficult to manage in time as new vendor equipment/protocols are added. Changes to the protocol of an individual line of equipment are no longer independent of the network in which the equipment is deployed, since such changes must be reflected through the various protocol conversion schemes.

Migration - Open Standard

As before, EM modules are required for legacy plant, this time however, they are used to interface to an open protocol as shown in Figure 5. Once an open protocol is available, the need for further proprietary protocols is reduced, eliminating "protocol creep".

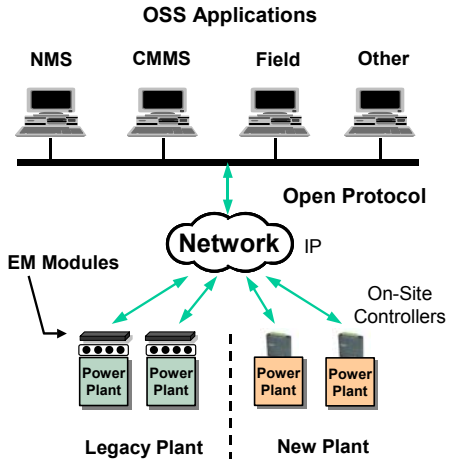
Figure 5 – Intelligent Monitoring, Open Protocol



With the availability of an open protocol, vendors have the option to make it available in new product offerings, this will not happen if the protocol is owned by a competitor. This reduces the cost of NMS deployment for the telco with off-the-shelf software interface modules from the NMS vendor. A migration based on an open standard promotes reduced cost in EM modules for legacy plant, encourages the development of new equipment with a conforming interface and reduces the proliferation of multiple protocols.

In the future the existence of an open protocol will encourage the development of OSS applications since these will each have a wider market base than is possible with many proprietary protocols. This is shown in Figure 6.

Figure 6 – Application Diversity, Open Protocol



As an example, consider readily available enterprise network management applications. These applications come as standard "out of the box" compatible with all the major open protocols because there is world-wide demand. However, if a protocol adaptor or a customized interface module is required (e.g. to a non-standard protocol), these can be expensive to purchase ($USD thousands or $USD hundreds of thousands), and software vendors may be reluctant to carry out development unless they foresee world demand.

In summary, telepower management systems that are migrated with the benefit of open protocols have many of the attractive features found in simple legacy systems operating on alarm terminal strips including:

- Simple for vendors to implement, low-cost.
- Set points and features may change internally for different applications or markets - protocol stays the same.
- Every power system has one.

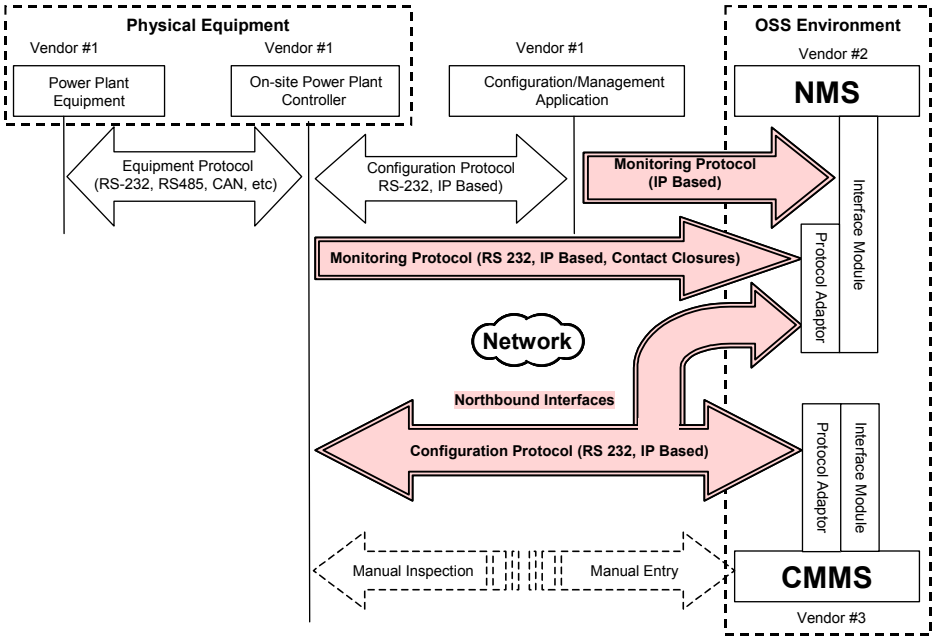
IV. WHAT TO STANDARDIZE & THE PROCESS

In considering what should be standardized, we need to consider the various information flows that occur between telepower systems and the telco's OSS environment. Much of the information that flows in the telepower system is proprietary (see Figure 7). This means that once information crosses from one vendor system to another there is a cost of integration involved. This typically requires a costly investment in the development of either physical protocol adaptors or software interface modules.

The Northbound Interfaces in the telepower network have the most potential to be standardized, as this would reduce the cost of integration. The protocols used along the Northbound Interface that would benefit from standardization are illustrated as doubled outlined arrows in Figure 7. These are the monitoring and remote configuration protocols. When these protocols are standardized the process of integration becomes simpler and more cost effective. This also increases opportunities for the automation of data transfer into management systems reducing the need for error-prone and time-consuming manual entry.

There is an argument that low-level equipment protocols should also be standardized, to allow for the inter-operability of power plant equipment. This type of standardization poses many more challenges and is not considered here.

Figure 7 – Protocol Layers



The type and characteristic of Northbound information required by the different management systems varies. For example the type and characteristic of information required by:

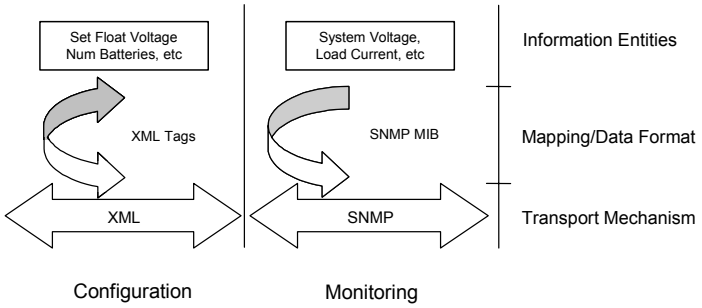
- A NMS *from* a telepower system is typically alarm and status information. This information must be available in real time and is dynamic. It's security profile is low as it is read-only, but it must be reliably delivered and have high integrity.
- A CMMS *from* a telepower system is typically system configuration and parameters, historical and performance information. This information must be available in real time but the CMMS does not require it to be instantaneously updated. Its' security profile is low as it is read-only, but it must have high integrity. If it is not reliably delivered it can always be requested again.
- A CMMS *to* a telepower system is typically system configuration and parameters. This information must be delivered in real time but is relatively static. It's security profile, reliability and integrity are all high as this information can change the state of the telepower system.

These different characteristics suggest that more than one standardized protocol may be needed. This will influence how a data standard is formed, in that it should not depend on one protocol technology. Another advantage to not limiting a standard in this way is that it allows future protocol technologies to be accommodated.

To support this concept, the framework for a standard could be based on a layered approach, where the definition of information being exchanged between systems is separated out from the transport mechanisms. This layering is shown in Figure 8:

- Definition of information entities (what information is required and it's representation).
- Specification of the transport mechanisms (what protocol should be used for what information flow).
- Mapping of the information entity definitions to the transport mechanisms.

Figure 8 – Standard Layers



To achieve standardization of all layers in one step may be ambitious. It would be more practical to consider each layer in turn. This approach has the advantage of allowing a flexible regime for compliance, where a vendor could reach higher levels of compliance over many product development cycles. The level of compliance could be:

Level 1: Monitoring - Notification Management.
Level 2: Monitoring – Status Monitoring.
Level 3: Configuration - Settings
Level 4: Configuration - Control

For example - Level 1 could be as simple as defining SNMP Traps similar to the RFC 1628 - UPS Management Information Base.

A survey of transport mechanisms (Ref [2]) used in network monitoring is shown below. When considering the characteristics of the main information flows in the Northbound Interface, that is remote monitoring and configuration (see Figure 8), two potential mechanisms are SNMP for simple monitoring and XML for advanced remote configuration.

SNMP – Simple Network Management Protocol SNMP has become a widely accepted interface of choice for IP based network management systems. SNMP is functionally simple, not arduous for equipment vendors to implement and easy for end-users to deploy. For efficiency the exchange of data is in machine format.
XML – Extensible Markup Language XML has become a widely accepted interface of choice between "technologically disparate management systems", because it allows for "separation of content of data from it's presentation and describes the content in terms of the type of data". It is human readable, is readily implemented and easy for end-users to deploy.
TL1 - Transaction Language 1. TL1 protocol is widely used in telco SONET data switch equipment as a machine-to-machine interface but is human readable. The Telcordia OSMINE certification process is expensive and time consuming to achieve.
CMIP – Common Management Information Protocol CMIP provided a well structured object-oriented approach to Network Management. It has not been widely supported in either OSS systems or data switch equipment. CMIP requires substantial processing resources to operate in a piece of equipment.
CORBA – Common Object Request Broker Architecture CORBA technology was investigated as a replacement for CMIP. It too, is based on a well structured object oriented approach to information exchange between systems. It was not adopted as an interface between OSS system and data switch equipment, but is widely used as an interface between OSS Management Systems.

V. WHAT MAKES A SUCCESSFUL STANDARD?

Time and time again in the technology arena competing standards emerge, but only some become ubiquitous. The ubiquity of a standard is not necessarily based on technical excellence, but on other less prestigious factors.

This has certainly been the experience in the realm of network management protocols. The Common Management Information Protocol (CMIP) is superior to the Simple Network Management Protocol (SNMP) in it's object-oriented design and "mechanisms for access control, user authentication and auditing" (see Ref [1]). However, complexity, operational resource demands and the time for it to settle as an OSI standard saw the de-facto standard of SNMP become dominant in the monitoring of IP connected devices.

Some of the factors that lead to a successful standard are as follows:

- *Market demand* – a need for such a standard by end-users such as telcos. If there are not clear issues of inter-operability and inter-connection between systems supplied from different vendors, then a telco is likely to tolerate proprietary protocols.
- *Clear commercial benefits* – there must be clear benefits for both the vendor and the end-user. If a standard will reduce the cost of integration of a telepower system to an OSS environment, then the availability of telepower equipment that is compliant to the standard may drive telco purchasing decisions. These decisions would also be driven by the simple fact of the standard compliant equipment being cost competitive compared to non-compliant equipment in terms of the total cost of ownership. A vendor is unlikely to implement a standard in their telepower system if it is not going to drive sales of equipment.
- *Vendor and end-user cooperation* – a standards committee should have a clear vision of what it is to achieve in a given time frame, and each member should be committed to achieving these goals. Members of a standard committee will always have vested commercial interests on behalf of their respective organizations. If these are allowed to dominate, the work of the committee will be impeded.
- *Short standardization development period* – a standard committee must have a clear focus that is driven by agreed milestones and timetable. A committee that becomes ensnared in endless technical debates, resulting in meetings that produce few results and consume hours of key engineering staff is likely to get relegated to history in these fiscally responsible times.
- *Efficient standardization process* – a standard of this kind is global in nature, so a standardization process that allows wide participation is required. The model used by the Internet Engineering Task Force (IETF) and working groups such as W3C should be adopted, where most transactions are performed by e-mail.
- *Simplicity, ease of implementation for vendors* – a standard that requires a short development cycle to implement is likely to receive quicker application in telepower systems. The certification process must also be simple so that compliance can be easily achieved, allowing the vendor to achieve rapid time to market. It is reported that "TL1 certification to Telcordia's OSMINE can cost vendors well over a million dollars and take over a year to complete." (Ref [2]).

For a standards committee to be established to successfully develop an open data standard for the telepower industry, these issues need to be seriously considered.

A standards committee needs an umbrella organization in which it can establish itself. The interfacing of the telepower systems into the telco OSS environment, means that telepower is moving into the IT domain and world of IP based networks. The working groups of the IETF have best served the standardization of data formats and transport of data in IP based networks. They have been able to respond in a field where technology is rapidly changing in an efficient and effective way. IETF standards have allowed the technology of the Internet to become ubiquitous, and would provide the same benefits to this standards initiative.

VI. TELEPOWER STANDARDS INITIATIVES

The call for an open data standard for telepower is not an original concept. There has been a body of work that has been built up over a period of time on this subject, but it has typically been done on a regional basis.

The results of a limited survey of the work that has been in the area of data standards/protocols related to telepower systems is shown in Table 1. This should not be considered an exhaustive survey but rather an over-view of what has been and is being done in this area.

Table 1 – Standards Activities

Year	Description
1993	ANSI T1.317-1993, Telecommunications - Uniform Language for Accessing Power Plants - Human-Machine Language *This standard does not seem to have been widely accepted or implemented.*
1996	YDN 023-1996 (Chinese) Specification of Supervision System for Power, Air Conditioner and Environment (Covers Intercommunicate Protocol and Intelligent Equipment Communication Protocol) *Application is limited to the Chinese market. The document is more a guideline of general requirements than an interoperability standard.*
2002	Major telepower vendors established a group to develop a SNMP RFC-MIB definition for DC Systems Power Supply for Telecommunication. *Agreement was not reached and the group was disbanded.*
2003	GR/CCM-01/01 Draft (India) Centralized Control & Monitoring System for Power Plants & It's Peripheries. *The Indian Telecommunications Engineering Centre is seeking to address the issue of centrally monitoring telepower sites that have a range of vendors' equipment. The standard addresses both new and legacy systems.*
2003	TELKOM SPECIFICATION SP2066 Requirements for Telkom SA Ltd Element Management Systems, Sub-Network Management Systems, and Network Element Manageability *Telkom South Africa requires telepower vendors to comply with the Telkom data network specification for the management of network elements in their OSS environment.*
2004	T1E1.5/2003-004R1 Draft Standard for Telecommunications Power Systems Management. *A T1E1.5 group has begun to consider what entities should be considered in a human-to- machine and machine-to-machine interface standard for DC Power Systems.*
2004	ITU - Open Communications Architecture Forum Focus. *International Telecommunication Union set up a new focus group to address issues arising from interoperability between products from diverse equipment and software vendors used by service providers. Ref [3].*

The authors of this paper call for a more international approach to be taken and for both vendors and end-users to be involved in the establishment of an open standard with a clear focus on the end-user.

VII. CONCLUSIONS

This paper has demonstrated the need for a global, open telepower standard. This need has been heightened by the growing trend and interest in intelligent network monitoring and configuration. It has been shown that telcos will benefit from an open standard through reduced costs, greater interoperability between vendor systems and applications, and better "future-proofing".

Due to a number of factors including the ready availability of open protocols, data standards and cheap hardware, the time is right to consider the formulation of an open telepower standard.

POSTSCRIPT

The authors of this paper seek non-commercial expressions of interest for the formation of a standards committee made up of both telcos and vendors. It is envisaged that some discussions may take place at Intelec 2004. Enquiries can be directed to Silcar or RTP via the above mentioned addresses or via the RTP Intelec 2004 booth #403.

REFERENCES

[1] "S 2.144 Selection of a suitable network management protocol". Bundesamt für Sicherheit in der Informationstechnik 2000.
http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm/s/s2144.htm

[2] "White Paper, Element & Network Management With Transaction Language 1 – TL1", Krishna Sanjeeviah, Neil Butani. AdventNet Inc.

[3] "ITU group to target software standards for networks" Posted on May 20, 2004 - A Web-only article from www.rcrnews.com