MODEL BASED, DETAILED FAULT ANALYSIS IN THE CERN PS COMPLEX EQUIPMENT

M. Beharrell, G. Benincasa, J.M. Bouché, J. Cuperus, M. Lelaizant, L. Merard
PS Division, CERN, CH-1211 Geneva 23, Switzerland

Abstract

In the CERN PS Complex of accelerators, about a thousand pieces of equipment of various types (power converters, RF cavities, beam measurement devices, vacuum systems, etc.) are controlled using the so-called Control Protocol. This Protocol, a model-based equipment access standard, provides, amongst other facilities, a uniform and structured fault description and report feature. The faults are organized into categories according their severities and are presented at two levels, the first being global, and identical for all devices, and the second being very detailed and adapted to the peculiarities of each device.

All the relevant information is provided by the equipment specialists and is appropriately stored in static and real time databases; in this way a unique set of data-driven application programs can always cope with existing and newly added equipment.

Two classes of applications have been implemented, the first one is intended for control room alarm purposes and the second is oriented for specialist diagnostics. The system is completed by a fault history report facility permitting easy retrieval of faults which have occurred previously e.g. during the night.

INTRODUCTION

The control system of the CERN PS Complex, with its nine separate accelerators, deals with thousands of pieces of equipment of various types and having different control sequences from each other.

The maintenance of such a quantity of hardware requires the use of an appropriate set of tools that, on the one hand provides a detailed specific fault report system, possibly organized in a hierarchical structure, and on the other provides uniformity in the presentation of information. The Mean Time To Repair (MTTR) a device is in fact strongly dependent on the clarity and unambiguity of the information (fault messages) that is sent by the device and that must be interpreted by the maintenance team.

A particular aspect in the fault recovery treatment concerns intermittent faults, i.e. those usually having non-destructive effects and that occur at certain moments and disappear before appropriate treatment can be undertaken. The cumulative effects of these faults can be dangerous because they often precede some major problem in the device; the fault hunting system must then provide adequate tools for detecting and reporting these.

Finally, different faults occurring in the same device or in separate devices can be connected with each other or have the same root cause The detection of the relationship between different faults is greatly helped by appropriately flagging fault messages with time information.

All these considerations have been taken into account in the design of the fault report system presented in this paper.

1. THE PS COMPLEX CONTROL ENVIRONMENT

The nine accelerators of the PS Complex are controlled using the same unique architecture [1]. The control system is based on the so-called “standard model” for controls, i.e. an architecture having two (or three) levels of computing, interconnected by an appropriate LAN.

The first level is composed of powerful workstations running under UNIX and connected with each other and with the second level through an Ethernet LAN using TCP/IP. At the second level we find a series of VME crates (called Device Stub Controllers, DSC) housing 32-bit processors of the 680xx type and running LYNXOS RT. For certain kinds of equipment a third level of control is used, based on field buses.

Software access to the equipment is performed through standard control modules called Equipment Modules (EM) [2] ; these modules, one for each type of equipment, are housed in the DSCs, and hide to application programs all the intricacies of the control system. A large ORACLE database is housed in a dedicated server and contains all the necessary information to run the accelerators [3].

In order to improve the access speed at run-time, two subsets of this database are extracted:

- Data Base Real Time (DBRT) is housed in a local server (one per accelerator) and contains, amongst other information, the addresses of all controlled pieces of equipment
- Data Table (DT) constitutes an essential part of the EMs and is thus housed in the DSCs and contains all the information necessary to control each single piece of equipment physically connected to that DSC.

The Alarm System [4] periodically scans (polls) all the equipment of the Complex and reports to the workstations the faulty situations. In this context has been installed some years ago the so-called Control Protocol [5, 6], a model based uniform access procedure for equipment. All the equipment of the PS Complex has been classed in families, each family containing the devices having similar goals and characteristics (power converters, RF Cavities, beam diagnostic instrumentation, vacuum systems, etc.). For each family behavioral static and dynamic models have been defined and the corresponding control and acquisition parameters have been identified.

The implementation of the Control Protocol is based on two separate software packages exchanging appropriate control and acquisition messages. The first, one package for each family of devices, is hardware independent and is realized in the form of an Equipment Module permitting access to all the equipment of the same family. The second, one package for each single device, is strongly hardware dependent and implements all the control sequences peculiar to this device. The two packages are largely independent each other and can be written by the most appropriate persons; only the exchanged control and acquisition messages must conform with the Protocol rules, i.e. contain the parameters identified in the concerned equipment model, expressed in an appropriate formalism.

In the equipment models and, as a consequence, in the contents of exchanged messages the identification and report of fault conditions has received particular care.

2. THE FAULT DESCRIPTION IN THE CONTROL PROTOCOL

In the Control Protocol the faults or, better, the anomalous situations, are described at two levels:

- the level, called QUALIFIER, is a global description common and identical for all families
- the second , called DETAILED STATUS, is specific for each piece of equipment

The QUALIFIER contains six indicators, not exclusive each other, in increasing order of severity:

- WARNING indicates a minor fault not having consequences on the behavior of the device. Nevertheless, it may indicate the beginning of some more serious condition.
- BUSY only indicates that the device is executing some time-consuming task, e.g. a motor is still running or some sub-piece is warming-up to the correct temperature, etc. The Busy condition is accompanied, where possible, by indication of the number of seconds necessary to terminate the action.
- RESETTABLE FAULT indicates that a major fault has occurred and prevents normal behavior of the device; the recovery from this fault can usually be obtained by executing a computer controlled reset that tries to restart the hardware and software of the device.
- NON RESETTABLE FAULT indicates that a major fault has occurred, similar to the previous one, but that no recovery action by computer is possible and that the specialist must be called.
- INTERLOCK indicates that a fault occurred not directly in the concerned device but in an interconnected system, and that this fault prevents the normal behavior of the device. An example is a bad vacuum condition which can prevent the measurements in a beam diagnostic device.
- INTERNAL COMMUNICATION fault (not present for all devices) concerns those devices having distributed hardware interconnected with a local network.

These Fault indicators provided by the Qualifier often represent sufficient information on the status of the device for the operators in Control Room. On the contrary they do not contain enough information for the device specialist or for a more precise diagnostic. In fact each indicator is the sum of several possible faults of the same category: for example, the Resettable Fault indicates that one or more resettable faults occurred, without indicating which ones. The DETAILED STATUS indicators answer this need.

Five of the fault indicators of the Qualifier (the Busy indicator has not been considered) have been detailed in order to contain up to 32 different causes of a fault. The number 32 is not magic, it is just sufficient in the PS control system environment. The 5 x 32 Detailed Status indicators are specific to each piece of equipment, and in general their meaning is different from one device to another. The specialist on each device defines the meaning of the 32 indicators for each category of fault, organizes them in increasing order of severity and provides appropriate error messages for each. A check is done by the controls specialists in order to avoid too cryptic messages or ambiguities, e.g. two messages referring to the same fault or two faults having the same message. Each of the fault categories is flagged with a timestamp indicating the time of occurrence of the most severe of the reported faults.

The Qualifier information is implemented in the PS control system as six (five for certain families) bits of a word contained in every acquisition message from a device. In this way, at each acquisition one has global information on the status of that device. The Detailed Status information is obtained with a specific request and comes as a special acquisition message containing, amongst other information, five (or four for certain families), 32-bits words, each bit representing a particular fault, Fig. 1.

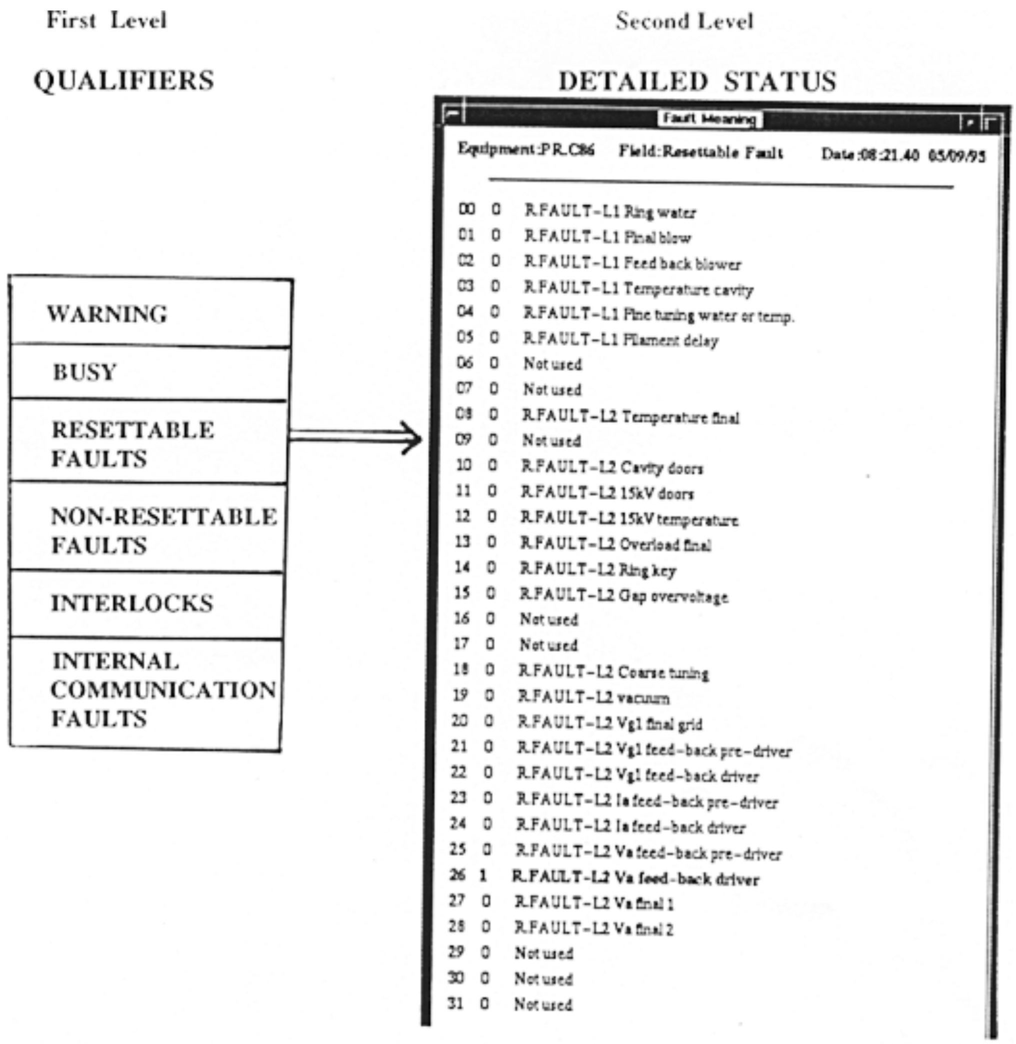

Fig.1 The two levels of the Fault report system (ex. a RF Cavity)

3. DATA BASE CLASSIFICATION OF THE FAULT INFORMATION

All the necessary information for the Fault report system is contained in two separate databases. A complete list of fault messages for all the PS Complex equipment is housed in the DBRT. The messages are stored and numbered in progressive order as they are provided by the equipment specialists; adding new messages is then a simple operation. Each message starts with indication of the category (Warning, Resettable fault etc..).

Appropriate functions exist that, given the fault number, retrieve the corresponding message. To date, about 400 fault messages are stored. The information specific to each device is housed in the corresponding Data Table in the concerned DSC. This information is stored in the form of 5 (4) groups of 32 integers, one group for each one of the previously mentioned categories of faults. The 32 integers in each group correspond to the 32 possible fault messages defined by the specialist for this specific category and for this device; each integer contains the number of fault message stored in the DBRT, as mentioned.

4. THE FIRST LEVEL OF APPLICATION - THE ALARM SYSTEM

As mentioned, the Alarm System periodically polls the various devices of the PS Complex and reports the anomalous situations in the form of short messages on the consoles. In the case where the polled device belongs to that class accessed by the Control Protocol, first of all the global fault descriptor Qualifier is acquired.

If one or more of the fault indicators are lighted, the function “Firstfault” is called. This function:

i) scans the Qualifier descriptor to identify, amongst the fault indicators, the most important in order of severity,

ii) interrogates the concerned device to obtain a Detailed Status Message, such as previously described. Among the 32 bits of fault in the selected category of indicator, it identifies the most important,

iii) finds the error message number corresponding to the position of the identified bit in the Data Table of the concerned device,

iv) retrieves, using this number as an input parameter the corresponding Fault Message from the DBRT and displays it on the console.

In this way the most important fault, amongst the 5 (4) x 32 possible fault conditions in this device, is displayed to the operator by the Alarm System.

5. THE SECOND LEVEL OF APPLICATIONS - THE DETAILED STATUS ACQUISITION

After a fault has been signaled by the Alarm System, somebody, either the specialist or the maintenance person, needs more information about the status of the concerned device. In this case the Detailed Status program is requested. This application is totally data driven in the sense that all the necessary information is contained in the DBRT and in the Data Tables - no new code or compilation is necessary when equipment is added or deleted in the accelerator complex.

In the example of Fig. 2 the case of a beam current transformer (TRAFO) is reported:

i) the application first searches in the DBRT to identify all the equipment families in the concerned accelerator using the Control Protocol facility; the complete list is then reported on the display,

ii) after the user has selected a family, the application searches once again in the DBRT for all the VME crates (DSC) containing the concerned kind of device and displays the list,

iii) the user clicks on the name of the DSC containing the hardware of the faulty device. By using the DBRT-stored information, the names (in the example beam transformers) of the concerned devices are displayed on the screen,

iv) finally the selection of the name of the device causes the request of a Detailed Status Message from the concerned hardware. This message contains (in this case) the 4x32 bits of fault information, as previously described. At this point the experienced specialist recognizes the various faults present in the device, often just by looking at the position of the set bits in the message,

v) otherwise, he can click on one group of 32 bits to obtain the messages on the display. To do this the application uses the information contained in the DBRT and in the Data Table, as already explained for the Alarm System. The complete list of the 32 fault messages is displayed, where the messages corresponding to actual faults are displayed in bold characters.

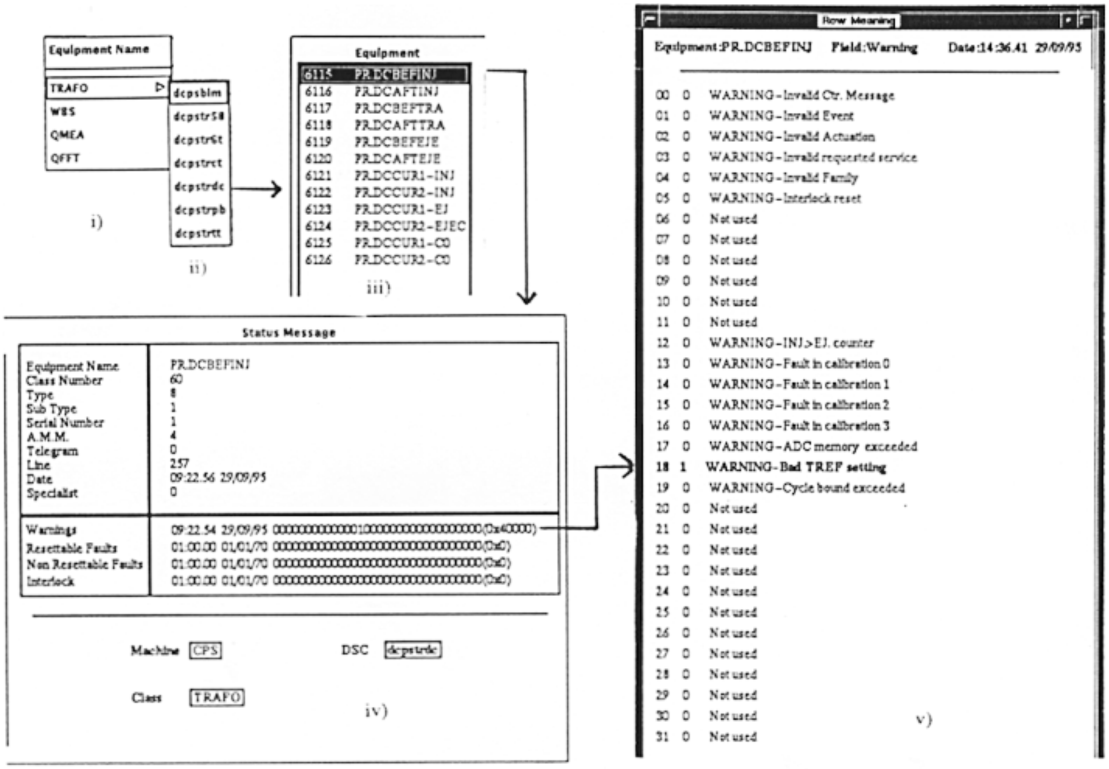

Fig. 2 The sequence in the Detailed Status application

6. THE FAULT HISTORY APPLICATION

As mentioned in the Section 1, certain faults are volatile and others are resettable by the operator before the specialist for the concerned device can be informed of their occurrence. On the other hand, it could be very useful to keep track of such faults for subsequent investigations. For this reason the Fault History system has been created.

The system is composed of two separate entities: a real time task, and an appropriate application. For various reasons, not reported here, almost all the devices of the PS Complex have a real time task, running in the corresponding DSC, and executing, among other activities, a periodical (~ 1.2 sec) acquisition of the relevant parameters which are subsequently stored in the Data Table.

For the devices using the Control Protocol facility, a complete acquisition message is acquired. In this case, when the specific software of a given device recognizes the occurrence of a fault that needs to be recorded, it sets an appropriate “look at me” flag in the next outgoing acquisition message. The real time task, after recognition of this flag, issues a request for a Detailed Status Message to the emitting device. The message with a timestamp is subsequently stored in an appropriate area of the Data Table organized in the form of a FIFO ring buffer. One such buffer exists per family of devices and per DSC:; it is presently sized to contain 100 Detailed Status Messages. In this way we have the complete record of the last 100 fault situations which have occurred, with their times.

The application program starts in the same way as described in i) and ii) of the previous section. At this point, by selecting the appropriate DSC name the program interrogates the ring buffer for this DSC and for the concerned family of devices, and displays the list of the recorded faulty elements with time, in chronological order. From this point on the program behaves in the same way as for iv) and v) of the previous chapter, the only difference being that now the Detailed Status messages are extracted from the ring buffer and not requested directly of the device.

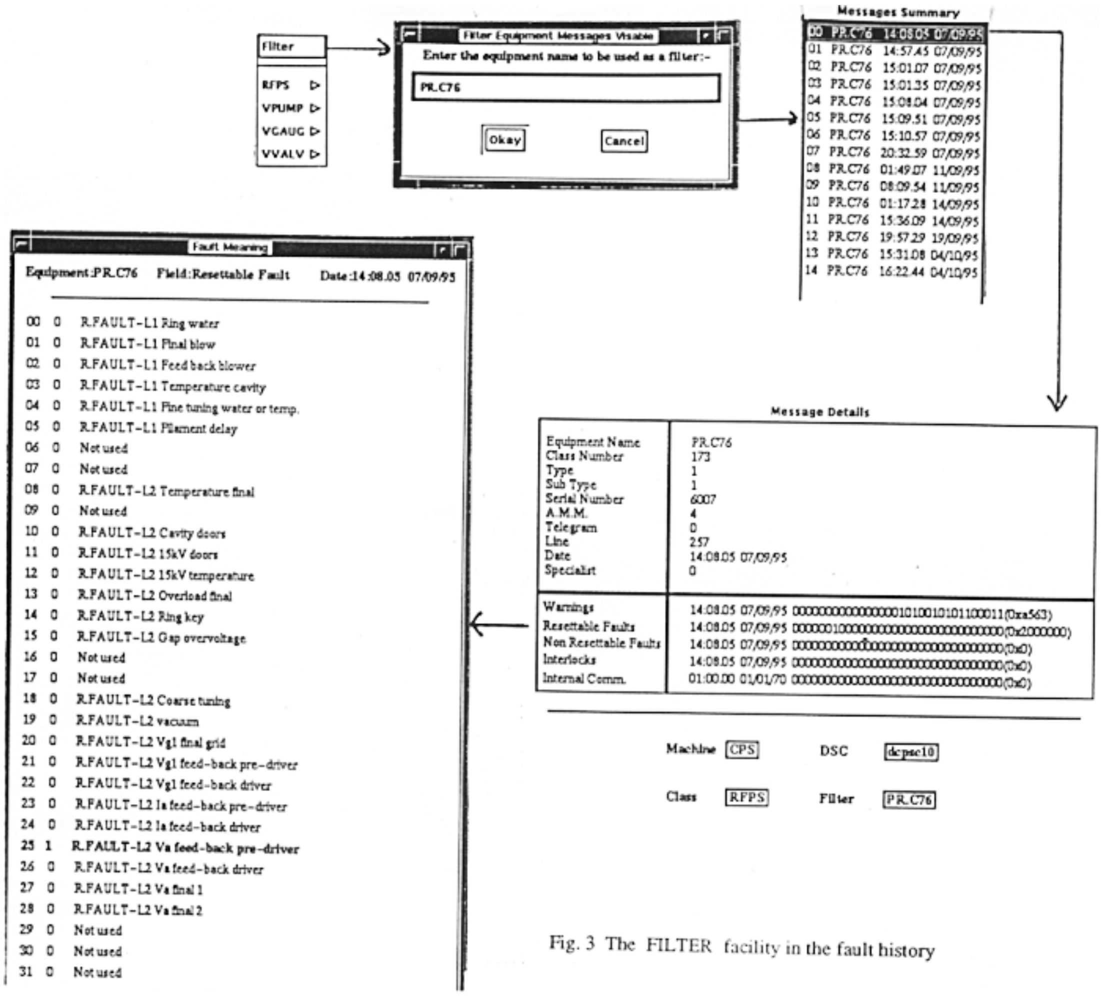

Fig. 3 The FILTER facility in the fault history

A useful feature, called Filter, permits easy following in time the fault behavior of a single device; to do this the user has only to provide the name of the inquired device, Fig. 3. The program searches the ring buffer and presents to the user a list of all occurrences of fault situations for the same device, chronologically organized. By examining the successive Detailed Status messages the specialist can extract important information on the fault's evolution.

7. CONCLUSIONS

In the PS Complex there are to date about a thousand pieces of equipment and devices using the Control Protocol; of this quantity, about half are thus far equipped with Detailed Status reports.

The presented standardization in Fault Reporting has proved to be a good compromise between the application of rules and constraints needed by any standard, and the necessity of implementing it in the accelerator environment where the variety of devices has in effect no limits.

The constraints have been limited only to the classification of the faults and in the formalism of their representation. This is especially appreciated in the control room where the operators receive information from thousands of devices. On the other hand, the equipment specialist is free to define the faults to be reported, the order of their severity, the corresponding fault messages, and that fault that should be recorded in the history.

REFERENCES

[1] F. Perriollat, C. Serre, “ The new CERN PS control system; overview and status”, ICALEPCS ‘93 , Berlin, Germany, October 18-23, 1993, Nucl. Instr. And Meth. A352 (1994) 86.
[2] J. Cuperus, W.Heinze, C.-H. Sicard, “ Control Module Handbook”, Version 4, CERN Internal Note PS/CO 95-01, 1995.
[3] J. Cuperus, “ The database for accelerator control in the CERN PS Complex”, IEEE Conference on Particle Accelerators, Washington, D.C. , March 1987.
[4] J. M. Bouché’, J. Cuperus, M. Lelaizant , “ The data driven Alarm System for the CERN PS accelerator Complex”, ICALEPCS ‘93, Berlin, Germany, October 18-23, 1993, Nucl. Instr. And Meth. A352 (1994) 196.
[5] Reported by G. Benincasa, (USAP Members: G. Benincasa, O. Berrig, P. Burla, A. Burns, P. Charrue, G. Gelato, R. Keyser, K.-H Kissler, T. Linnearc, F. Perriollat, J. Pett, M. Ranany, C.-H. Sicard, P. Strubin), “Final report on the uniform equipment access at CERN”, CERN Internal Report PS 93-16 (CO), 1993.
[6] G. Baribaud, I. Barnett, G. Benincasa, O. Berrig, R. Brun. P. Burla, R. Cappi, G. Coudert, C. Dehavay, B. Desforges, R. Gavaggio, G. Gelato, H.K. Kuhn, J. Pett, R. Pittin, J.P. Royer, E. Schulte, C. Steinbach, P. Strubin, D. Swoboda, N. Trofimov “ Control Protocol : the proposed new CERN Standard access procedure to accelerator equipment - Status Report”, ICALEPCS ‘91, Tsukuba, Japan, KEK Proc. 92-15 (1992) 591.