OPTIMIZATION OF ADVANCED PLANTS OPERATION : THE ESCRIME PROJECT

C. Fiche, B. Papin
CEA/DRN/DER/SSAE
CE Cadarache, 13108 St Paul lez Durance Cedex, France

ABSTRACT

The CEA has started a research work concerning the improvement of safety in operation for future plants. In order to minimize the impact of human errors, design and organization of the operational layout for control room operation is of major importance. In that domain the Escrime program aims at defining the optimal share of tasks between humans and computers under normal or accidental plant operation.

Basic principles we keep in mind are the following : human operators are likely to be necessary in the operation of future plants because we cannot demonstrate that plant design is error free, so unexpected situation can still happen ; automation must not release the operators from their decisional role but only help them avoiding situations of cognitive overload which can lead to increase the risk of errors ; the optimum share of tasks between human and automatic systems must be based on a critical analysis of the tasks and of the way they are handled.

The last point appeared to be of major importance. The corresponding analysis of the French PWR's operating procedures enabled us to define a unified scheme for plant operation under the form of a hierarchy of goals and means as presented on figure 1. Different kinds of tasks are distinguished : at the upper level plan management tasks with feedback and anticipation mechanisms; at mid level, management of essential functions taking into account eventual conflicts between the different functional goals ; at the lower level tasks like system configuration, starting or stopping component, ...

Beyond this analysis, development of a specific testing facility is under way to check the relevance of the proposed plant operation organization and to test the human-machine cooperation in different situations for various levels of automation. The facility (fig. 4) consists of an EDF 1300 MW PWR plant simulator connected to an operator workstation with interactive graphic display. Architecture of the surveillance system is part of the project, the goal being to have an alarm system coherent with the plant operation organization. The software architecture follows an artificial intelligence approach.

1. INTRODUCTION

In parallel with a large program aiming at the definition of severe accident management measures both for prevention and mitigation of accident consequences, the CEA has started a research project concerning the improvement of safety in operation for future plants.

In the frame of this research project this paper is concerned by the part named "ESCRIME" [1], the aim of which being to minimize the impact of human errors in operation. The domain covered is design and organization of the operational layout mainly for control room operation, that is to say : basic principles of decision making, quality of procedures and operational guidance, nature and domain covered by operating aids, role of monitoring systems, ...

The allocation of functions to man or computer is a very critical choice to be taken. Testing the design concept on realistic simulation situations is essential before freezing the final decisions and this is the purpose of the ESCRIME project. The development of a testbench is under way to evaluate and optimize cooperation mechanisms between man and machine for nuclear power plants operation.

2. THE ESCRIME PROGRAM

2.1. Basic principles

According to [1], basic principles leading this project are now summarized.

The increasing automation of nuclear power plants may improve the overall level of operation safety. But all the operation tasks cannot be automated and we cannot demonstrate that plant design is error free nor that all possibilities of plant situations are covered by the operational procedures nor that measurements are all reliable. So unexpected situations can potentially occurs and therefore this ensures that nuclear plants will be still operated by humans for the foreseable future. The problem is then to determine the tasks the operator will have to do under normal and abnormal plant conditions : so the ESCRIME program aims at identifying the optimal share of tasks between human and computerized operation.

The results of probabilistic risk assessment (PRA) studies on existing plants, stressing the important impact of the human factor on the overall risk of core melt and so justifying the limitation of the decisional role of operators, can be considered to be somehow biased by the implicit hypothesis that the operational procedures are free of design error. In case of unexpected situations, uncompletely covered by procedures, the potential positive contribution of the operators is neglected. Roles of operators are reduced to those of an unperfect extension of these procedures, with the only alternative to follow them step by step or to fail.

In fact automation must not release the operators from their decisional role, but must only avoid situations of cognitive overload which lead to increase the risk of errors when taking important decisions. In case of important safety actions (as safety injection actuation), on the basis of PRA studies which show that errors or delays in the execution may lead to unacceptable consequences, automation has been choosen. It could be possible to give the operators more responsability considering that fundamental causes of cognitive overload is that operator's attention is often caught by tasks of secondary importance, hindering them to be fully aware of the particular importance of actions to be taken. Putting more emphasis on these "important actions" and avoiding they were hidden by numerous low level tasks, can be an alternate way to the systematic automation of all actions having a potential impact on the safety.

In case of increased automation of plant operation the human actor's role and technical skills has to be reconsidered in depth, instead of letting the operators face the uncomfortable situation of continuous shrinking of their domain of intervention. The decrease of operators involvement in terms of workload (number of individual tasks and actions directly handled) has to be compensated by an increasing importance of their decisional role : the future plant operators are likely to take high level decisions, making use of the improved capabilities of computerised support system (expert system, knowledge-base system), and will have less low level tasks to handle by themselves.

In the domain of support system and layout there is a strong need for the operators to perceive the feedback of their actions on the plant process in order to learn, improve and maintain their knowledge of the plant operation. A purely passive role in plant monitoring will lead to the loss of capabilities. More, it is essential for operator understanding not to hide physical phenomena and reactor behavior under many computerized program layers. The man-system interface will try to give a close representation of what occurs in the plant, presenting synthetized informations adequate to the present situation.

The search for the optimum share of tasks between human operators and automated systems must be based on the systematic critical analysis of the tasks to be achieved and of the way they are handled in the actual plant operating procedures. This analysis aims at identifying generic principles that could be used for a clearer formalization of the operating rules, and at searching for a better consistency of these principles, in the whole domain of plant operation.

2.2. Operation tasks analysis

Nuclear power plant (NPP) operation in most of the countries is based on quite similar basic principles, that can be drawn from the analysis of operating procedures.

The systematic sequentialization of tasks is due to the fact that most of them have to be performed by the same operator (who can handle a limited set of simultaneous tasks). Howewer, the functional

analysis of plant operation shows that it mainly consists in maintaining continuously and in parallel a limited set of important objectives (which are the critical safety objectives in accident management), instead of trying to satisfy them one after another. Our reflection on this point aims at reinforcing the execution of tasks in parallel, everywhere it increases the efficiency of plant operation. This mainly concern high level tasks. Low level sequences of actions, which contributes for example to the lining up of a hydraulic system, are of course to be executed in sequence. The execution of such actions could be made easier by implementing adequate automated functions managing each operational objective, while the operator intervenes in choosing the relevant objective to be maintained, depending of the actual status of the plant.

If normal operation has slightly evoluted refering to the state at the beginning of NPP and is mainly based upon a material component approach (system-based representation of the plant), abnormal operation, on the contrary, has been redefined in depth during the 80's as a consequence of TMI 2 accident. It changed towards a more function oriented approach, insisting upon the fundamental safety objectives to be filled in order to maintain the integrity of the barriers. Such an approach leads to a better structuration of the operation. So, our intent is to try to extend this principle to all the domains of plant operation. This will homogenize the operational practices, thus avoiding that the operator has to manage different mental models of the plant depending of the situation.

As said before, in the domain of accidental operation, the previously used "event oriented approach" tends to be completed or replaced by more generic operational principles based on the maintenance of critical safety functions . The strategical principles of this approach are clear and simple, potentially easy to understand and to be followed by operators, provided they are trained to this "function oriented" way of thinking. Nevertheless, the actual implementation of these principles in plants are still complex, because of the need to maintain a certain level of time optimization in the operation (thus leading to maintain a certain amount of event-based strategy or to look for short cuts in the application of general symptom-based principles). This is due to the fact that weak points in the design of plants of the actual generation do not allow for the use of straightforward strategies in case of emergency, because, for example, of a too short delay of decision. Concerning that point, we consider that the foreseeable adoption of more "forgiving" design principles will open the way to the generalization of simple management principles as safety function-based management and to the disappearance of too specific adaptations, introducing unwanted complexity in plant operation.

3. FUNCTIONAL ARCHITECTURE

The analysis of plant operation principles, mainly based upon French PWR operating procedures, leads us to define an unified scheme for normal and abnormal plant operation. It is a generalization of the state oriented approach defined by EDF for accident recovery to what we can call a function oriented approach. This scheme, presented on figure 1 describes and structures plant operation in a

hierarchy of goals to be satisfied and means to be used to achieve the upper levels goals. It is the basis for task allocation study between man and machine but it does not anticipate what will be the repartition or share of tasks between man and machine.

3.1. Main functions

The main functions presented in figure 1 are defined here :

Definition of the global goal : The global goal is defined from the following inputs :

- external demand, coming from the electrical grid management
- current state of the plant (in case of accident, a safe and stable state must be reached),
- output from planning function, which concludes that the desired state cannot be reached (for example, if a Xenon oscillation is occurring).

Generation of the global plan : this plan defines the successive operating phases that allows to reach the global objective from the actual state of the plant. The execution of a phase drives the plant to an intermediate state which, in normal operation, is one of the reference reactor states. The initial plan, that is generated a priori following the definition of the global objective, can be dynamically modifed in case of failure of a step or unexpected evolution of the plant.

Management of the global plan : In accordance with the global plan, this function determines the current goal to be satisfied by the lower functional levels. It uses informations on the plant state and on the results of previously active goals.

Management of the current goal : The current goal can split up into two sets of subgoals of different types :

- satisfaction of functional objectives (for instance primary water inventory control, criticality control, ...) which must be maintained continuously and simultaneously,
- satisfaction of systems configuration objectives which are related to put in (out of) operation the systems involved in the functional objectives (for example chemical and volume control system). These tasks are to be performed only once, as a pre-requisite condition for satisfaction of the current goal.

Functional objectives management : Functional objectives are to be permanently maintained, by means of elementary functions. The availability of those elementary functions depends upon the operational status of the main systems of the plant and the physical state of the process. A functional objective may be achieved in various ways by combination of elementary functions. This functional redundancy, which mainly exists on accidental situations, allows to find several paths to achieve a goal and thus to cope with elementary function failure.

Plant systems management : A plant system can support several elementary functions. A system can be out or in service. Going from one system state to the other, as asked by the system configuration objectives defined in the current goal, requires the execution of specific tasks (verification of a priori conditions, lining of hydraulic circuits, chemical and thermo-hydraulical conditioning, ...). These operations are generally linear sequences of well defined elementary actions on components. As a system can be required for several functions at the same time, conflict of resources is to be managed.

3.2. Main mechanisms

The general diagram presented in figure 1 can be transformed in a SADT like diagram such that is presented in figure 2. In such a diagram, tasks are placed in the boxes and links stand for information flow. At the general level of the representation, all of the tasks are executed in parallel.

The first task performs data acquisition and processing to give values of the main physical parameters and the status of systems and components. All these values are used by the following tasks (n° 2 to 5) whose names are identical to those of figure 1.

The n° 2 task, "global plan generation", determines the global plan in accordance with the external demand, physical and status data, and chooses the operating procedures to be applied. In such a representation task 2 is supposed to cycle and adjust the global plan in accordance with data. The explicit feedback from lower levels indicated on figure 1 is in fact implicitly present in the process data (physical and/or status).

Task n° 3, "Global plan management" determines the current goal for task n° 4 depending on the global plan and the set of procedures to be applied. As the previous one, this task is supposed to be determining continuously the right goal in accordance with the evolution of the process data.

Task n° 4, "Current goal management" determines a list of functional objectives corresponding to the current goal, with priorities of execution and criteria of success if necessary. Each of the functional objectives is broken up in elementary actions by task n° 5 (figure 3), "Functional objective management" which acts in parallel on the different objectives. Task n° 4 receives from task n° 5 an execution report in order to correctly manage the goal because, in certain conditions, different possibilities can exist to achieve it.

The functional objective execution report can inform about execution failure due to task's pre-conditions not satisfied or component failure or conflicts as defined hereafter.

- In fact pre-conditions, often attached to a task, must be fulfilled in order to be able to execute it. For instance, using low head safety injection for water inventory, requires that the primary pressure be lower than a given value.

- Execution criteria also, defined in terms of physical parameters values and status of components are needed to determine if a goal is sucessful or not.

- Moreover, at a given level in the goal hierarchy, when a failure occurs in the execution of the part of the plan relative to this level, an attempt can first be made to use physical or functional redundancies of systems and alternate elementary functions to determine an alternate success path. If it is unsuccessful, higher level goals must take the failure into account. In some cases, the global goal itself can be modified, for instance in accidental situation.

- Concerning conflicts, two kinds of situations have been identified. First, functional objectives can call for actions on elementary functions in opposite ways (for example cooling or heating). This conflict is solved by attributing priorities to the objectives depending on the physical state of the plant (this is done actually in French state oriented emergency operating procedures). The second kind of conflict appears when several elementary functions activated at the same time share the same system resources. The strategy takes into account the relative priority of the attached functional objectives and tries to find alternate paths. It is worthwhile noting that this situation is solved in existing NPP procedures. These conflicts indicate a common mode in the plant design, and thus potential safety problem. In future plants, the design tendancy is to assign one system to one function, so this type of conflict will be avoided.

3.3. Man-machine cooperation

Guidelines for allocations of functions which are synthetized in [4] can be applied within the frame of the ESCRIME functional architecture. The classification of functions in three levels (must be automated, are better automated, should be allocated to humans) defined in this document helps to the allocation of functions in ESCRIME. Low level sequential operations dealing with system configuration, continuous monitoring of large number of variables, anomaly detection through threshold passing, advanced monovariable regulations can easily be automatized (and so they are in several actual plants). They correspond to the lower levels of the structure presented on figure 1. The boundary is moving together with the advance in information technology. For intermediate levels, where " intelligent" decisions are to be made, it is mainly here that different share of tasks are to be evaluated. One important point is that it is not only to give a task to the operator and another one to the machine, but, and it is essential, to make them communicate and cooperate. This cooperation is a dynamical process. The operator can delegate, for a certain interval of time, a dedicated task to the machine. The machine can make suggestions to the operator. The operator will gain confidence in the machine if he is able to rebuild the automated reasoning in any case.

4. DESIGN

4.1. Facility architecture

The facility architecture is presented in figure 4 where the higher part represents the simulator and the lower part the ESCRIME testing bench. This part can be seen as organized around a central node which is an information server managing data exchange between the various control and information processing tasks and the physical process representation. His organization enables the progressive introduction of new control functions depending on needs for the project. Presently, the choice of the software tools suppporting this organization is not definitively choosen. A multi-agent software architecture could be convenient as shown in section 4.2.

The development on a SUN workstation of a first version of the structure presented in figure 3 is underway with a software tool developped in CEA Saclay for prototyping.

4.2. Multi-agent architecture for dynamic planning

The operation of a plant by operators can be represented as a problem of dynamic planning of actions in a moving environment. Distributed Artificial Intelligence techniques seem well adapted to modelize this activity, as it deals with artificial systems that are in fact distributed.This approach is very convenient and flexible and the mechanisms provided are dedicated to represent cooperation and communication between "entities", that is a major point in the ESCRIME project. In particular, this formalism makes the allocation of different tasks to the operator very easy.

The scope of agents definition can be very large, from physical components to abstract systems or "specialists". The possibility of making more detailed and complex the behavior of an agent, to modify the task allocation to agents and to add new agents, without modifying the overall design structure, is very well adapted to test different modes of man-machine cooperation.

The functional architecture presented in section 3 can be viewed as the straightforward specification for a multi-agent implementation. The design follows the multilevel representation. A goal is assigned to each level, where a set of agent is active to achieve the goal. As an example dealing with the current goal management level, functional objective agents cooperate in order to achieve the current goal. They delegate their task to elementary function agents which are available. In case of conflict, functional objective agents negotiate and can report to the upper level if no agreement has been reached.

4.3. Operator interface

The operator interface plays of course a major role in ensuring an optimal cooperation between man and system. Its design must be driven by the informational needs of the activity, and not only by the technology available at this time. The design, which is actually in progress, takes profit of the development and testing of the computerized procedures for the N4 type control room [6]. The underlying principle is to give to the operator the right information at the right place and at the right

time. The operator will be presented at any time a synthetic view of the plant state and of the status of the global operating objectives and he can ask for more information.

As for the global design the multi-agent technique can be directy applicable here, the interface being defined as a set of agents which react to events and adapt dynamically their behavior to the situation.

4.4. Plant simulation

The ESCRIME workstation is connected to the modular simulation code CORIANDRE [7] which is oriented towards the detailed representation of control interface with the plant : sensors, actuators, automatic control. This flexible tool provides facilities for the representation of auxiliary and safety reactor systems as CVCS and SIS, loosely coupled to the main plant systems, but playing a prime role in the plant operation. Special attention has been payed to the representation of power supplies, in order to be able to represent complex and realistic combination of components and systems failures.

5. PROJECT STATUS AND FUTURE DEVELOPMENTS

A first version of the prototype is expected for the middle of 1995. It will implement the mechanisms described in section 3, on a limited plant domain and systems representation. Low level tasks dealing with system operation will be automatized. The different ways of man-machine cooperation that will be tested will be defined, alltogether with the evaluation criteria and the specification of relative comparison tests on simulator.

In further steps, concerning the higher levels of management of figure 2, we will attempt to elaborate the strategy on line instead of applying logical rules already existing in the present procedures which, as said before, describe chaining of actions without giving adequate strategy explanation to the operator.

Furthermore the system could extend to the whole plant domain and go deeper in the area of detecting and recovering the dysfunctioning of the automatics and of the plant. The use of physical models (quantitative or qualitative) for anticipating the operation will be looked for. An other domain of research will be the communication between man and machine, for example by giving to the computer system capabilities of operator intent inferencing from his actions on the plant.

6. CONCLUSION

The ESCRIME project main objective is to define the role to be played by the operator in the operation of future nuclear power plants, through the evaluation of different allocations of tasks between man and machine on a dedicated workbench. This project is not independent from other

themes of investigation in the domain of instrumentation, hardware and software control (how to implement reliable systems and how to prove their reliability ?) and of plant design, but it is a step that cannot be skipped when designing future plants.

REFERENCES

[1] B. PAPIN, A. POUJOL, 1991

Development of advanced operator workstations for future plants : status of the reflection in the CEA., in Proc. of IAEA/OECD International Symposium on Nuclear Power Plant Instrumentation and Control, Tokyo, 1991

[2] L. BAINBRIDGE, 1983

Ironies of Automation, Automatica, Vol. 19, N° 6, pp 775-779, 1983

[3] B. PAPIN, P. MALVACHE, 1994

Evolution of the future plants operation for a better safety, in Proc. of International.Topical Meeting on Advanced Reactor Safety, Pittsburgh, 1994

[4] W.BASTL, J. JENKINSON, A. KOSSILOV, R.A. OLMSTEAD, A. OUDIZ, B. SUN, 1990

Balance between Automation and Human Actions in NPP Operation, in Proc. of IAEA/NEA Symposium on Balancing Automation and HumanAction in Nuclear Power Plants, Munich, 1990

[5] A. POUJOL, B. PAPIN, R. SOLDERMANN, 1992

Procedure Generation for Operator Assistance under Emergency Operation in Nuclear Power Plants, in Proc. of 8th Power plant Dynamics Control and Testing Symposium, Knoxville, May 92

[6] P. LE BOT, R. SOLDERMANN, G. GUESNIER, G. BELTRANDA, B. PAPIN, A. POUJOL, 1990

Development and Testing on a full-scope Simulator of Computerized Operation Procedures under Accident Conditions for the New Control Room for EDF's New1400 MWe SeriesPWR, in Proc. of IAEA/NEA Symposium on Balancing Automation and Human Action in Nuclear Power Plants, Munich, 1990

[7] P. DUFOUR, 1990

OASIS and CORIANDRE : User friendly and flexible simulation tools for FBR's and PWR's, in Proc. ENS/ANS/FORATOM ENC'90, Lyon, France, 1990

Fig 1 : Generic global functional architecture for plant operation

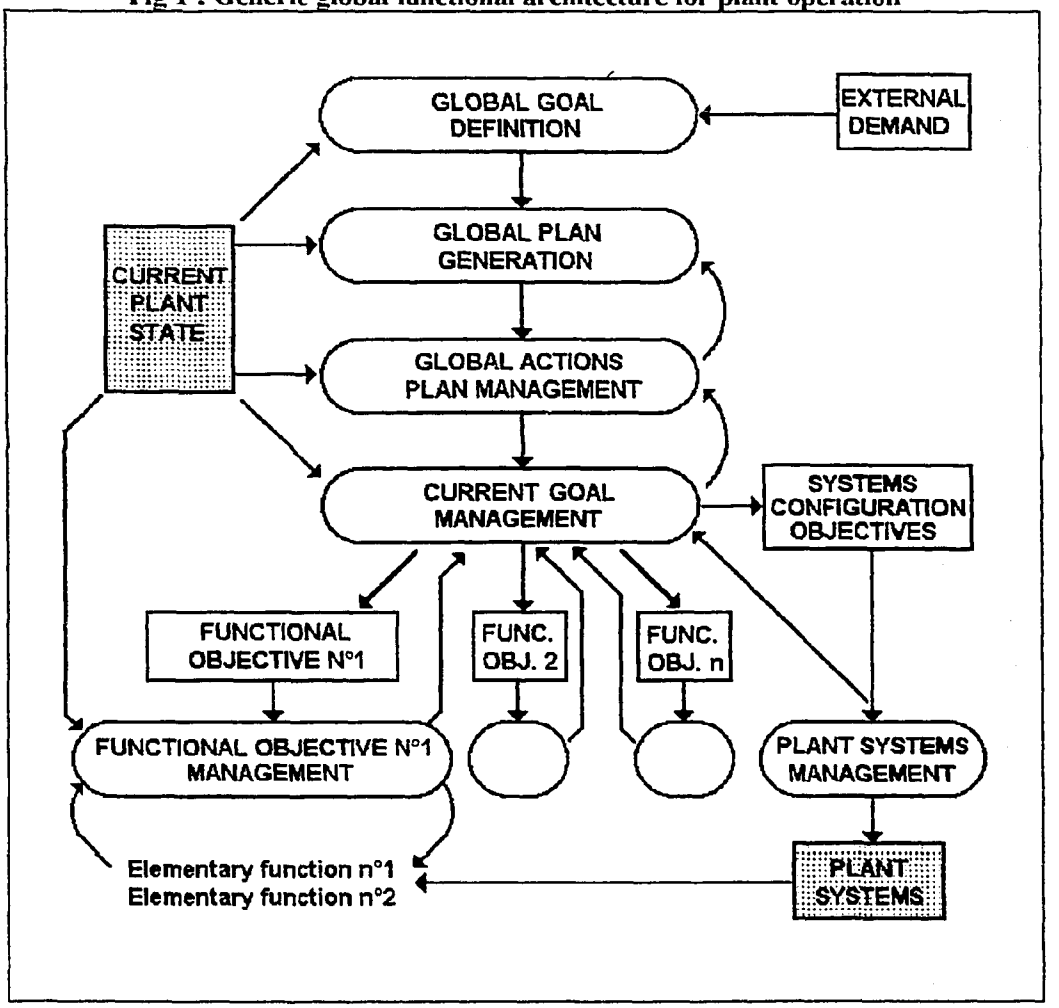

Fig 2 : General tasks diagram corresponding to fig. 1

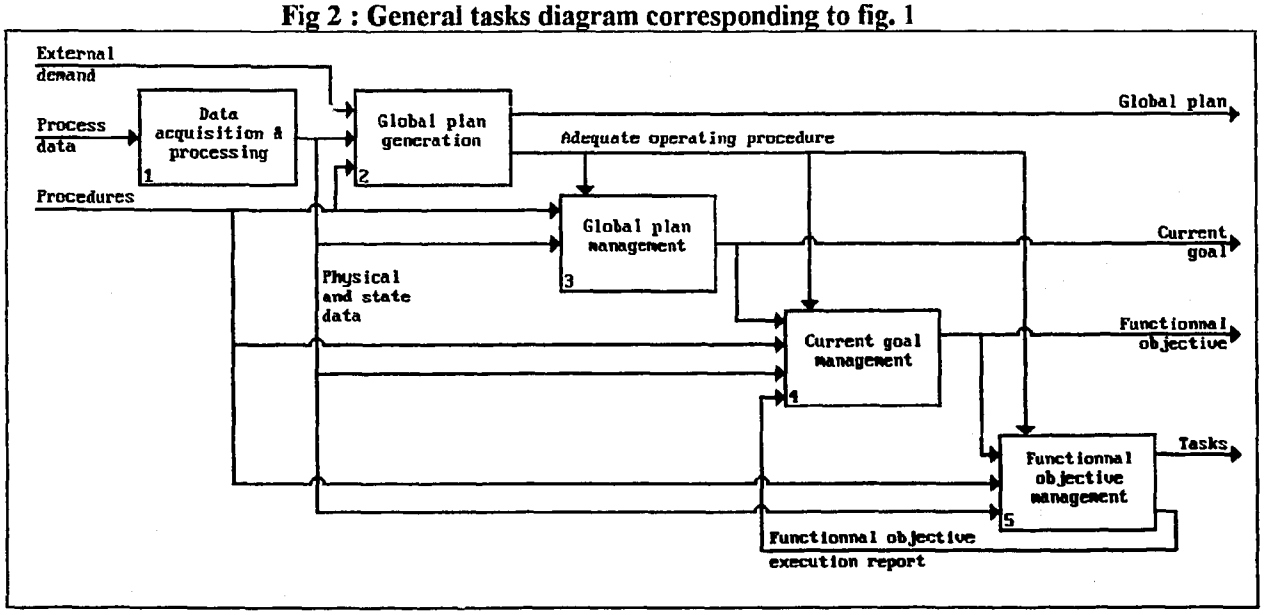

Fig 3 : Detail of task 5, fig.2 "Functional objective management"

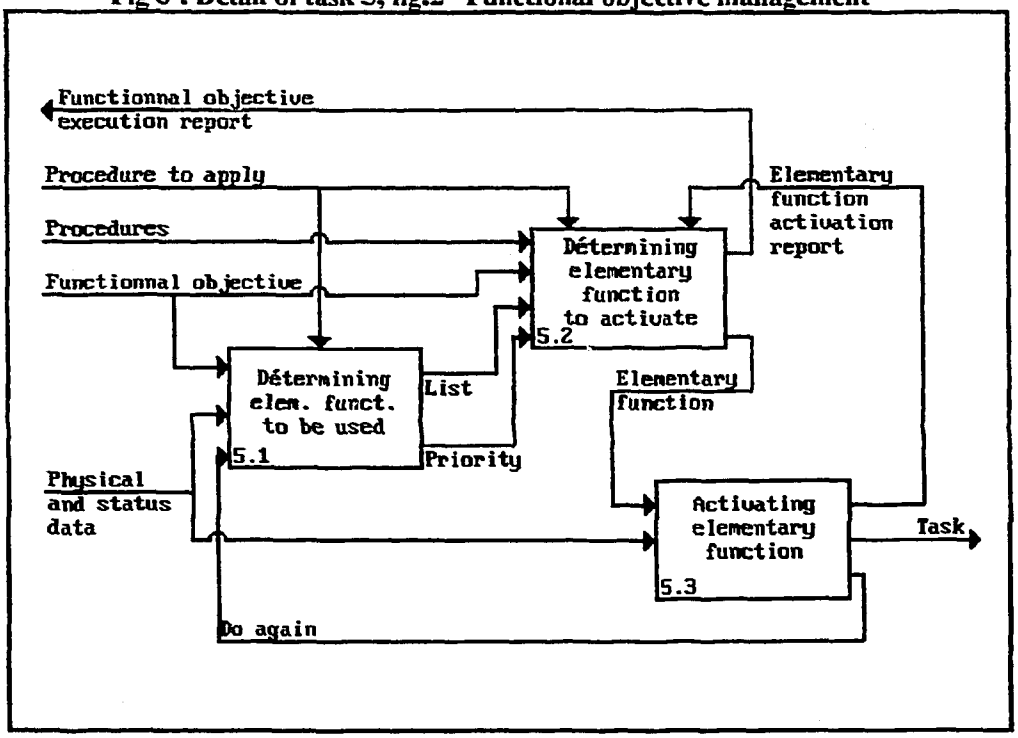

Fig 4 : ESCRIME facility architecture