Managing Abnormal Situations II: Collaborative Decision Support for Operations Personnel

Peter T. Bullemer, Ted Cochran, Steve Harp and Chris Miller
Systems and Software Technologies Department
Honeywell Technology Center

Introduction

The largest economic disaster in U.S. History (not due to natural causes) was a $1.6 billion at a petrochemical plant in 1989. This accident represents an extreme case in a gamut of minor to major process disruptions, collectively referred to as abnormal situations in this proposal. Most abnormal situations do not result in explosions and fires but are costly nevertheless, resulting in poor product quality, schedule delays, equipment damage, and other significant costs. The inability of the automated control system and plant operations personnel to control abnormal situations has an economic impact of at least $20B annually in the petrochemical industry alone (Nimmo, 1995).

The Abnormal Situation Management (ASM) Joint Research and Development Consortium, led by Honeywell, was formed in 1992 to develop the technologies needed to allow plant operations personnel to control and prevent abnormal situations. In addition to Honeywell, the ASM Consortium includes the U.S. operations of the seven largest petrochemical companies (Amoco, BP, Chevron, Exxon, Mobil, Texaco and Shell), two innovative real-time industrial process controls applications software vendors (Applied Training Resources and Gensym), and a specialty chemical company (Nova Chemicals). In addition, the ASM Consortium has three university affiliates in Dr. Jim Davis of Ohio State University Department of Chemical Engineering, Dr. Venkat Venkatasubramanian of Purdue University School of Chemical Engineering and Dr. Kim Vicente of University of Toronto Department of Industrial Engineering.

In 1994, the U.S. National Institute of Standards and Technology (NIST) Advanced Technology Program (ATP) awarded a 3.5-year, $16.6 million cooperative agreement to the ASM Consortium. The goal of the NIST-funded Collaborative Decision Support for Industrial program is to demonstrate the technical feasibility of collaborative decision support technologies for improving the performance of operations personnel.

This paper presents the system-level solution, AEGIS (Abnormal Event Guidance and Information System), currently under development in this NIST ATP program. We begin the discussion with a prototypical characterization of the nature of collaborative decision-making in the process operations environment of the petrochemical industry. Next, we present the collaborative decision support vision as characterized by six primary functional roles of the AEGIS prototype. In addition, we discuss several technological innovations addressing key challenges in collaborative human-machine interaction, system architecture, and system customization tools. Finally, we conclude with summary of program progress in implementation of the technical innovations and future research plans.

Collaborative Decision-making in Process Operations Environment

Most oil refineries and petrochemical plants use distributed control systems (DCS) to simultaneously control thousands of process variables such as temperature and pressure. The major human role in this control is to supervise these highly automated systems. This supervisory activity requires: monitoring plant status; adjusting control parameters; executing pre-planned operations activities; and detecting, diagnosing, compensating and correcting for abnormal situations. Increased demands for higher efficiency and productivity in these industries are resulting in tremendous increases in the sophistication of process control systems through the development of advanced sensor and control technologies. However, these sensor and control technologies have not eliminated abnormal situations and will not in the future. Consequently, operations personnel continue to intervene to correct deviant process conditions.

The persistent paradox in the domain of supervisory control is that as automation technology increases in complexity and sophistication, operations professionals are faced with increasingly complex decisions in managing abnormal situations. A contributing factor to this phenomenon is that the sophistication of the user support technologies has not kept pace with the task demands imposed by abnormal situations. Thus, the focus of this program is to develop collaborative decision support technologies that significantly improve abnormal situation management practices.

Decision making model for Operations Intervention Activities

To provide a decision making model with which to structure solutions to existing ASM problems, the ASM Consortium adopted a modified version of a model proposed by the Chemical Manufacturers Association show in Figure 1. This model provides a description of how a plant operations team responds to intervene in an abnormal situation. The left side of the figure represents the occurrence of an external abnormal situation. The operations team, represented by the dashed box, then will intervene to stabilize the process.

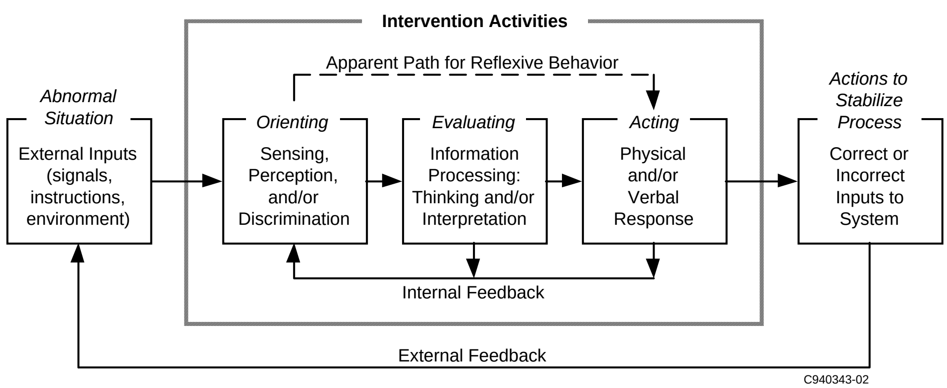


Figure 1. Decision-Making Model for Operations Intervention Activities

- **Orienting—**In the first stage of intervention, a disturbance in the process is detected. In the Evaluating stage, the operations team develops hypotheses regarding the cause of the anomalous operating conditions.

- **Evaluating**—As denoted by the dashed line, which goes directly from the first to the third stages of intervention, responses to certain disturbances may be so well-rehearsed that it may appear that the Evaluating stage is skipped.
- **Acting—**Finally, the operations team must make compensatory and/or corrective action, including actions to determine if the hypotheses are correct.

All preventable abnormal situations can be traced to a breakdown in the intervention activities (For detailed discussion, see Cochran & Nimmo, 1997). For example, external inputs pertaining to process upsets can be missing, erroneous, or masked—which leads to incorrect orienting and subsequent behaviors. The fundamental goal in developing AEGIS is to improve ASM by enhancing the accuracy, completeness, and speed of the human activities in Orienting, Evaluating, and Acting.

Plant Operations Roles

There are various operational and nonoperational personnel that impact the operation of a process unit in a plant complex.

The plant personnel fulfilling the operations shift team roles are expected to be the primary users of the AEGIS functionality. A prototypical operations shift team consists of a shift leader, a console operator, and 2-5 field operators. In general, shift teams work together, unless someone is out sick or on vacation, in which case another shift team member comes in to cover for him. Shift teams rotate from working nights to days. Most shifts are 12 hour periods. During the weekdays, many maintenance projects are going on, and the engineers, craftsmen, management personnel are all available to interact with the shift team. The night, or “graveyard” shift is a completely different story. Very few people are around and the goal is to “survive the shift”, i.e., to keep everything going until morning. If an upset happens, there are no backup people available, so the shift leader has to call in help if there is time.

- **Shift Leader—**The shift leader role (also known as the head operator or stillman) is responsible for overseeing the field and console operators in the detailed monitoring of the process and ensuring the execution of the relevant preventative maintenance (e.g., daily routine duties) and abnormal situation management responses. The shift leader is a senior operations staff member, who may or may not be qualified as a console operator (although they typically are qualified). The shift leader is in charge out in the field. He typically makes “rounds” in the field as a follow-up to the field operator’s rounds, observing the process equipment and making minor adjustments, noting potential equipment problems, and verifying sensor readings. He is also responsible for filling out the “Shift Log Book”, which is a written log located in the shed, describing any significant activities that have taken place during his shift. During an upset, the shift leader becomes another hand in the field, generally playing a secondary role to the console operator who is in control. If there is sufficient time, the shift leader will get on the phone to call for backups.
- **Console Operator—**The console operator is responsible for controlling the process via the distributed control system. He/she has the task of monitoring and making “moves” that maintain and change the state of the process. In addition, the console operator has the responsibility of coordinating the actions of field operators and keeping abreast of the

maintenance activities in the field. The console operator is the focal point of communication between the various distributed operations personnel throughout the complex because he has the central view and control of the process via the DCS. A console operator must first be certified as an field operator in all field areas.

- **Field Operator—**Depending on the size of a given unit within a plant, there will be one or more field operators. Each operator is responsible for their own area but many are qualified on more than one area (they may rotate from one area to the next, and they monitor each other's work, by keeping an eye on the other areas as they conduct their rounds, and sometimes helping another operator when performing maintenance and/or troubleshooting tasks). Some of the field operators are also console operator qualified, and may rotate from working in the field to working in the control room every other day. The field operator has the equipment view of the process and serves as the "human sensor" that checks the status and validates the correctness of the sensor and instrumentation readings in the field to ensure that the view of the process is accurate. In addition, field operators use their senses (e.g., eyes, ears, and nose) to monitor the process, constantly identifying potential problems (a funny smell or sound) with the process equipment and initiating preventative maintenance, adjustment, and repair activities. Field operators take periodic readings of indicators not available to the console operator, take periodic product samples for laboratory analysis by the process engineers, and perform manual operations such as operating soot blowers or operating manual valves. Field operators prepare and warm up equipment such as steam pumps and place them on line in a controlled manner to avoid sudden surges, cavitation, or loss of suction. They are responsible for directing maintenance personnel to the appropriate worksite and for receiving deliveries of products (such as catalyst) to the unit. In an upset situation, they are the first on the scene and provide a critical diagnostic and mitigating response role in abnormal situation management by assessing the situation (e.g., confirming/refuting DCS data) from a process equipment perspective and by taking actions which are outside of the scope of DCS control either by design (e.g., fire fighting) or by circumstance (e.g., slide valve stuck, controller broken). In an upset situation, the console operator may need assistance, and one of the field operators working in the field who is also console-qualified will go to the control room as quickly as possible. The other field operators and the head operator must cover in the field in his absence.

Other plant personnel influence the operation shift teams intervention activities and at times are directly involved in the response to an imminent or existing abnormal condition. Brief descriptions of these roles are provided to give the reader an indication of extent of collaborations among diverse roles in the process operations environment. These other roles include:

- **Shift Coordinator—**The shift coordinator (often referred to as shift supervisor). plays the role of operations team coordinator and management interface between the operations superintendent and the operations staff. He is responsible for monitoring the process and its impact on the unit's daily production targets. In addition, he is responsible for high level coordination of the console and field operations staff in meeting production goals, completing preventative maintenance, and coordinating abnormal situation responses as well as working with maintenance and instrumentation staff in prioritizing and executing lock out, tag out (LOTO) and maintenance activities.

- **Operations Superintendent—**The operations superintendent is responsible for the productive and safe operation of the complex for which he is responsible (i.e., a complex is typically run by multiple shift teams). The areas of responsibility include monitoring and reporting of the budget and costs associated with complex operations, safety reporting and documentation, environmental compliance and incident reporting, training, and production reporting to upper plant management. He is responsible for tracking high level plant operational goals and is ultimately responsible for meeting those goals
- **Site Planner—**The operations planner in some cases may represent a team of people where each is responsible for different areas of plant. A planner is responsible for tracking possible market opportunities (e.g., high demand, high price, scheduled shipments, weather conditions) that may arise along with planning for expected maintenance and turnarounds (I&T).
- **Process Engineer—**The process engineer(s) is responsible for generating the daily production orders for each process unit within a plant which are developed by the site planner. The process engineer troubleshoots process unit problems and determines why they are not making plan from a process (as opposed to an equipment) perspective
- **Control Engineer—**The control engineer is process and economics knowledgeable. S/he maintains control tuning, control objectives, and develops and implements improved control. The control engineer often troubleshoots process and control related problems after operations has stabilized the process. This troubleshooting often depends heavily on historical databases and anecdotal information from operators.
- **Maintenance Coordinator—**The maintenance coordinator (also referred to as supervisor or foreman) is responsible for coordination of maintenance activities for the plant units. The maintenance coordinator schedules periodic preventive maintenance, and maintenance requests put in by the operations team. S/he will determine the resource requirements, order any required materials, and determine if any contractors need to be hired to perform the job.
- **Maintenance Technician**—Instrument or mechanical technicians are responsible for maintaining and repairing all the process equipment.

Collaborative Decision Support Vision

The purpose of AEGIS is to support the plant operations team in achieving the four high-level objectives of ASM:

- Keep the process operating normally;
- *Failing this*, restore the process to normal operation;
- *Failing this*, bring the process to a safe state;
- *Failing this*, minimize severity of any accident.

To support operations in achieving these objectives, AEGIS needs to work with the operations staff to recognize abnormal situations, correctly diagnose problems, plan the best course of action, and carry out the plan correctly and efficiently.

Six Functional Roles. The AEGIS collaborative decision support vision is presented in Figure 2. The vision depicts AEGIS as six major functional roles referred to as: *State Estimator*, *Goal Setter*, *Planner*, *Executor*, *Communicator*, and *Monitor*. Briefly, the State Estimator role provides a concise dynamic estimate of what is actually happening in the plant, including trend information that may be used to predict future states. The Goal Setter examines the result and proposes a prioritized agenda of high-level goals to pursue. The Planner creates a plan to achieve those goals given the current plant state. The Executor carries out the plan, ensuring that each step is executed at the right time. The Communicator manages the interface between the other Roles and the plant personnel. The Monitor examines the operation of the other Roles and regulates their activities accordingly.

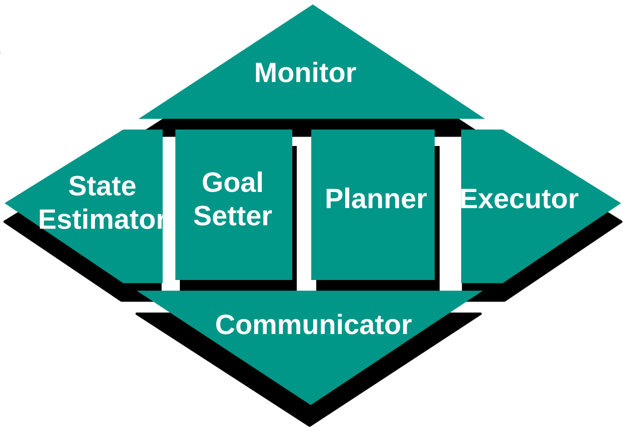


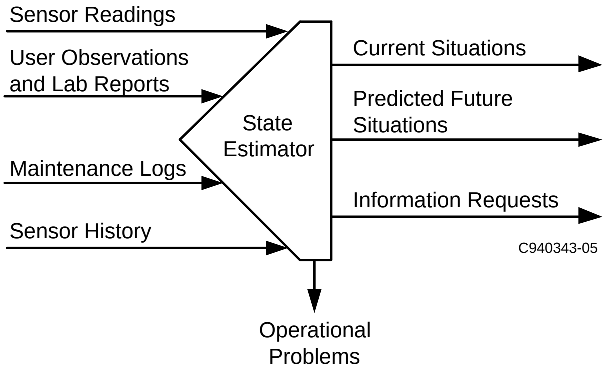
Figure 2. AEGIS Functional Roles

The following six sections describe AEGIS operation by discussing the individual functional roles. For each role, we discuss what it does and why this is important to solve the ASM problem. We also discuss how the role works and how it interacts with the other Roles and users.

The State Estimator Role

What it Does. The State Estimator provides a concise and dynamic estimate of what is actually happening in the plant. It reduces the torrent of sensor data available on the DCS every second to a narrow stream of explanatory states we refer to as *situations*. Situations attempt to capture the necessary and sufficient information to assess the health of the process and the equipment in the plant. The scope of the estimator encompasses the complete process area supervised by a single console operator along with major interactions with upstream and downstream process areas. This would include the mechanical condition of the process equipment, the maintenance activity within the area, the process control applications and systems, and the refining/chemical process itself. The estimator receives sensor inputs and historical information directly. Other relevant information needed as input (e.g., maintenance logs, operator observations, lab reports) can be accessed either from the communicator module (if these are available in an electronic form in different computers) or manually entered by the operations personnel.

The goal of the State Estimator is to explain as many plant events as possible with the smallest set of *situations*. A situation may represent a root cause of an abnormal situation, such as the failure of a piece of equipment or sensor, a process disturbance forcing control changes, a trend in process variables, or an incorrect manual intervention.



Situations are really a generalization of the notion of diagnosis, covering a wider range of explanatory levels. Some are quite specific. For example, the situation “Valve-32 is stuck in the 24% open position” is recognizable as a specific diagnosis. Other situations represent greater degrees of uncertainty, such as “Product quality from Tower-2 has been declining for the last hour.” This is better described as a high-level symptom than as a diagnosis, but it may be as much as can be deduced at an early stage of an abnormal situation. All situations derived by the state estimator are qualified by estimates of their certainty.

The State Estimator’s vocabulary of situations is defined by the needs of the other AEGIS modules. In essence, the situations of interest to AEGIS and to plant operators are those that may make a difference in plant operations. For example, instead of continuously presenting sensor measurements from the operation of a distillation tower, the State Estimator might condense sensor information to conclude that the liquid level in the tower was “too high to support *X*” when (and only when) *X* was a planned operation—and would pass along pertinent data to other AEGIS modules for planning and communication purposes. Generally, pertinent situations such as “pressure relief valve about to release” would always be monitored.

The State Estimator has several outputs. It is primarily responsible for deriving current situations—the instantaneous position of the process and equipment. However, with enough knowledge, predictions of future situations are also possible. Predictions are likewise qualified with certainty and time frame. The state estimator may be able to identify specific information it needs to make a better assessment; these are passed on as information requests. Finally, the State Estimator may be able to detect when it is failing. Such operational problems are also a form of output and are of interest to the Monitor Role.

How it Helps. The State Estimator impact on the ASM problem is made through the speed and accuracy of identification and diagnosis of existing or impending abnormal situations. The preventive detection and diagnosis of sources of abnormal situations will increase the time available for performing compensatory and/or corrective operational activities. Quick identification of abnormal situations and predictions of future abnormal situations allow operators to take compensatory actions before the problems escalate. A later explanation may contain the root cause description needed for a corrective action.

The AEGIS environment provides plant situation assessments from the State Estimator to the operations team by way of the Communicator module. Suggested remedial actions also are forwarded by the Goal Setter, Planner, and Executor.

How it Works. The AEGIS State Estimator incorporates a synthesis of some of the most successful approaches to sensor-based diagnosis and sensor validation, as demanded by the domain. In particular, we incorporate elements of heuristic methods as well as those based on models. Heuristic methods use the "compiled" knowledge of domain experts. Model-based methods use a model of the device or process being diagnosed along with a more generic reasoning method to derive a diagnosis.

Heuristic methods are fast and do not require a plant model, but are comparatively brittle—they cannot handle situations that were not explicitly anticipated. Model-based techniques are less brittle, but pose other problems. Most industrial chemical processes are unique. Consequently, it is difficult to build high-fidelity first-principles models of these processes and very difficult to anticipate what abnormal situations are common. Very few processes are amenable to theoretical modeling.

A complicating factor is that the sensors and actuators used to control the plant also fail, and not infrequently. One approach to sensor failure is to use redundant sensors and select a reading based on a majority vote or some combination. This technique has been widely used in the aerospace industry. Industrial process control operates under different economic constraints, and the application of triply redundant sensors is usually unrealistic in today's plants or in designs for the near future. In the absence of physical sensor redundancy, analytical redundancy (i.e., observer-based schemes) can be used to monitor the entire system—actuators, sensors and equipment—and capitalize on redundant information available in collections of different sensors.

One of the technical innovations we provide in the AEGIS State Estimator architecture is a framework that enables several of these promising techniques to work effectively together.

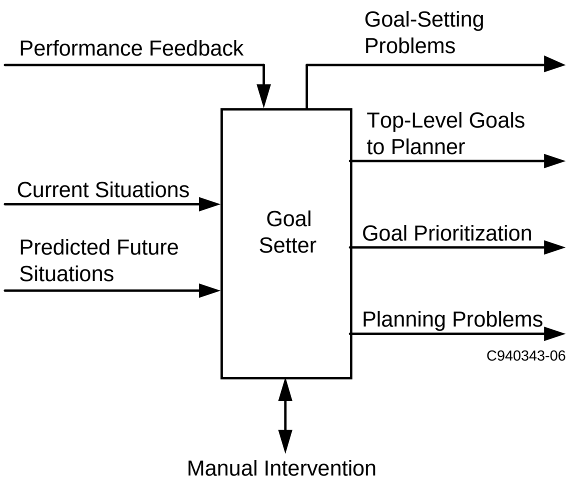
How it Interacts with Other Roles. The State Estimator provides fundamental information about plant health that is used by all of the other Roles. Although it receives its primary input from plant sensors (via the DCS) and users, it also accepts instructions in the form of requests for information or situation assessment from all of the other AEGIS modules. These may involve controlling its adaptation or allocating its resources.

Through the Communicator, the operations team members can interact with the State Estimator in various ways, including:

- Inspecting state explanations.
- Entering information not available through the sensor network.
- Directing an analysis of some specific data.
- Defining new state explanations for particular data patterns or relations.

The Goal Setter Role

What it Does. The Goal Setter examines the situations provided by the State Estimator and proposes a prioritized agenda of high-level goals to pursue. The goals are passed to the Planner to find the best way to achieve them. Because not all goals are simultaneously compatible or appropriate at a given time, the goal-setting process involves making some executive decisions about priorities and resources. These are based on external considerations in the context of the projected impact on process, plant equipment, and safety. For example, safety-related goals may cause production-related goals to be deferred in some situations.



Key functions of the Goal Setter include:

- Identifying desired changes to the process state (target or safe situation to achieve).
- Finding alternative situations (in case the optimal one is unattainable).
- Assessing the future risks of the present situation.
- Evaluating the relevance of currently active goals.
- Setting the agenda for the Planner.
- Prioritizing goals and setting deadlines.

How it Helps. Critical problems confronting operations teams are communicating current operational goals, identifying the impact of goal modifications on operational objectives, and making consistent tradeoff decisions given multiple objectives.

The explicit representation and prioritization of goals in the AEGIS Goal Setter improve the consistency and efficiency of operations. Plant personnel can track tradeoff decisions and receive feedback on the impact of goals on abnormal situations. Allowing operations staff to interact with the goal-setting process helps their understanding of the plan and enables them to work better as a team.

How it Works. The Goal Setter must convert a set of identified situations into a set of goals to achieve. In the simplest case, a situation corresponds to a unique and certain diagnosis of a known problem. For example, the situation might be “Runaway reaction in vessel 7.” The possible goals addressing this situation may be retrieved from a situation-indexed data/knowledge base. In the example, the only sensible goal may be “Quench runaway reaction.” Information may also be retrieved about the expected costs and resources required for dealing with the situation, and the time course and consequences of not dealing with the situation. Continuing the example, it may be noted that quenching the reaction might take the process off line for anywhere from 2 to 4 hours, and that failure to quench the exothermic reaction in the next 15 minutes could ruin the $100,000 reactor.

As noted, goals may interact in a positive or negative way. In some cases, the interaction between goals may be known to the Goal Setter. The “quenching” goal might be known to be incompatible with a goal to increase production from this vessel. In other cases, the interaction could be more subtle, and the Goal Setter would rely on the Planner and the operator to detect negative interactions between proposed goals. For example, part of the quenching procedure may demand cooling water that is urgently needed elsewhere in the plant. The planner communicates these as “planning problems” to be resolved by the Goal Setter.

Part of the Goal-Setter’s job is managing uncertainty. Uncertainty enters from the assessment of the current plant situation and from forecasts of future events. Suppose, for instance, the situation “Runaway reaction in vessel 7” was diagnosed by the State Estimator with likelihood 0.125. Given these odds, should the Goal Setter launch a “Quench runaway reaction” goal?

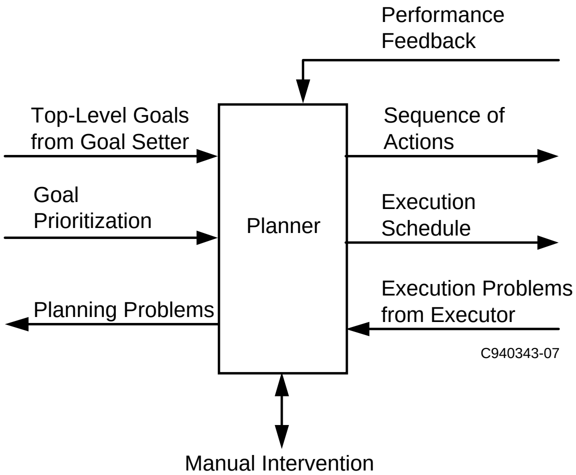
Another Goal Setter responsibility is noting when the motivation for a goal disappears. Some problems are corrected without the completion of a planned remedial action. This occurs since AEGIS cannot know all possible causal relations in the plant; the situation can be resolved for unknown reasons, or the operator may have had other means to solve the problem. In such a case, the goal setter needs to establish a goal to safely abandon a plan that may be under way. This may entail “clean-up” actions (e.g., restart halted equipment).

How it Interacts with Other Roles. As primary communications links, the Goal Setter receives situation information from the State Estimator via situations posted on the shared AEGIS blackboard. It provides an agenda to the Planner. The goal agenda can contain new situations to be monitored and these may need to be conveyed to human operators for approval or revision. Thus, as secondary communications links, pertinent aspects of the goal agenda are conveyed to the State Estimator and to the Communicator. The operations team members are able to interact with the Goal Setter by:

- Viewing the current prioritized agenda of goals.
- Asserting, modifying, or retracting individual goals or priorities if so authorized by plant management.
- Receiving feedback on the impact of prioritized goals on plant productivity.

The Planner Role

What it Does. The Planner takes the high-level goal agenda from the Goal Setter and generates a plan to satisfy it. The plan is elaborated as a partially ordered set of simple actions to be carried out by the Executor. The Planner uses special reactive techniques, since speed is essential to react to urgent situations.



Key functions for the Planner include:

- Finding and scheduling a sequence of actions that satisfy all goals on the agenda.
- Detecting negative interactions between plan steps.
- Resolving choices between alternative courses of action (feasibility, risk, cost).
- Calling for diagnostic tests or other information required for planning,
- Determining key variables to monitor (especially process constraints) and their time profile while trying to execute goal sequences.
- Verifying plan steps to help monitor the plan success.

How it Helps. Abnormal situations are often caused or worsened by the application of inappropriate procedures. The Planner generates action plans, appropriate to the current situation, which can be modified as appropriate by the operations team. Over time, the system adapts to the specific planning needs of the operations team and improve the adequacy of procedures to ensure better responses to abnormal situations.

How it Works. The Planner adapts the best of emerging technologies to fit the real-time demands of this domain. Although there are many approaches to plan generation, including table lookup, task reduction, macro-operators, and planning from first principles, the real-time nature of the ASM planning problem and the need for replanning as the situations change imposes special constraints. Traditional task reduction (hierarchical planning) would require enormous knowledge-engineering task effort. The consequences of integrating different schemas in real-time plans are difficult to anticipate. Planning from first principles requires modeling of individual, atomic actions and makes it harder to encode effective guidance on how to construct good plans. These problems can be eased significantly if we can work with partial models and rely on users to critique plans of action.

From analysis of existing plant procedures, we believe that successful planning in this domain can exploit a *procedure library*. In some cases, this could be as simple as a database of procedures indexed by situation. The procedures can be parameterized to handle variations in the equipment or resources involved (a limited form of context sensitivity), or could consist of fragments to be combined into a plan or hierarchy of task “schemas” describing how to accomplish tasks under certain conditions. Each of these approaches has limitations, but good balance may be achieved via a combination of complete procedures for the majority of conditions, with additional fragments incorporated as necessary. All of the plans are parameterized, and the Planner can incorporate operator assistance in constructing and critiquing new plans.

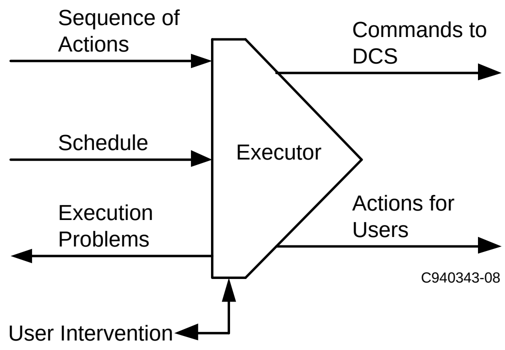
How it Interacts with Other Roles. The Planner receives a top-level agenda from the Goal Setter. It may also get deadlines for producing plans from the Goal Setter, forcing it to react in a timely fashion. The plans produced are passed to the Executor to be put into action. The Planner uses situation information from, and posts monitoring requests to, the State Estimator. The Planner may need to ask the Communicator for human authorization or modifications to suggested plans, and it may need information about the availability and whereabouts of plant personnel. When the Planner is incapable of producing a plan for a goal it has been given, the problem is reported to the Monitor or the Goal Setter as appropriate.

Operations team members are able to interact with the Planner to:

- View the current partially ordered action plan.
- Authorize, command, forbid, or halt individual plans if so authorized by plant management.
- Assert, modify, or retract actions or the order of actions in the plan.
- View/modify the scope of responsibility for individual resources within the plant.
- Receive feedback on impact of the action plan on plant productivity and abnormal situations.
- Define new action plans for specific goals in terms of alternative actions and constraints on use.

The Executor Role

What it Does. The Executor supports carrying out plans. It issues the lowest level commands that actually cause changes in plant systems: to plant actuators, to other automated systems via the DCS, and to plant operations personnel, such as field operators, via the Communicator module. The Executor, in conjunction with the Planner, constructs a detailed schedule of actions and, in conjunction with the State Estimator, monitors their performance to ensure that each step is carried out at the right time.



How it Helps. In addition to monitoring for failure of plant equipment to perform as expected, the Executor addresses a major source of ASM costs, failure to follow procedures. Human operators under stress can omit steps, add steps, execute steps out of sequence, enter wrong values without confirmation, and fail to confirm actions completed by another team member. When procedures are carried out incorrectly, remedial actions are required. Some simple remedial steps may be stored in the Executor itself; others may require more complex replanning, or revisions to goals involving the Goal Setter.

How it Works. The Executor requires detailed knowledge of procedures—how to perform plan steps in the operating environment of the specific plant. This must include knowledge about plant personnel and their capabilities and duties, and information about resources required to execute these steps, including time of personnel.

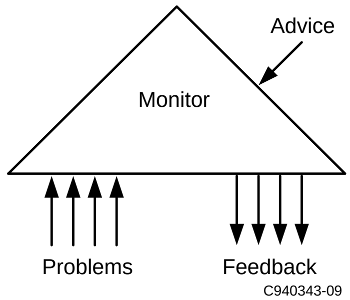
Execution error monitoring is more demanding. The Executor matches observed states to expectations. There are two general approaches. Reactive error trappers catch either bad states or unexpected actions once they happen. Proactive error trappers monitor for series of actions that lead to an “error pattern” and try to halt them along the way. The Planner may have anticipated certain failure possibilities and inserted explicit “plan-checking” steps.

How it Interacts with Other Roles. The operations team members are able to interact with this Role in the following ways in accordance with their individual privileges and responsibilities:

- Initiate and/or confirm action command execution.
- Modify allocation of actions to resources including between system and humans.
- Indicate status of actions requiring manual response outside of system observations.
- View status of action commands including verification of command reception.
- View command queue for individual resources within the plant.
- Prompt or remind operations team member on need to perform manual task.
- Verify appropriateness of action.

The Monitor Role

What it Does. The Monitor evaluates the overall effectiveness of the coordinated activities of the other Roles. The object of the Monitor is the rest of AEGIS, not the plant per se. It identifies bottlenecks and inefficiencies in overall system performance and provides feedback to the other Roles to allow AEGIS to automatically adapt and improve.



How it Helps. Some of the shortcomings in current ASM practices stem from a lack of reflection on how similar situations were handled (or mishandled) in the past. The AEGIS Monitor is a tool for evaluating the effectiveness of ASM practices. Through the tracking and documentation of ASM activities, operations personnel and AEGIS Roles are able to adapt and respond in a more effective manner to future situations.

A simple example of the Monitor in action involves improving the knowledge base of the Planner. Suppose the Planner assumes that pressure in a particular boiler can be reduced at the average rate of 50 psi/minute. The Monitor may notice that the last three times this procedure was attempted, the achieved rate was only 30 psi/minute. The Monitor could present such discrepant observations to plant personnel. Engineering might decide to the change the Planner or look for some other cause for the slower pressure release rate.

How it Works. The Monitor tracks activities of AEGIS in interaction with human operators by monitoring problems reported by AEGIS modules. It also monitors the statistics of normal inter-module communications. From this trace of plant operations, the Monitor attempts to detect internal problems and isolate patterns of suboptimal performance.

A key activity of the Monitor is to track success and failure rates for goals, plans, and actions. Plans and actions that routinely fail are inspected in more depth for either remediation or removal. The same sort of scrutiny applies to top-level goals that are routinely rejected by operations. A particularly interesting case exists when goals are met without a known plan succeeding. This implies either that an intermittent, self-repairing problem is present (an important trigger for planning and executing diagnostic activities) or, of more interest for the Monitor, that plant operators are using a plan or activities that AEGIS does not know about. In the latter case, machine-learning or knowledge-acquisition techniques can be used to acquire this novel plan and integrate it into the AEGIS knowledge bases.

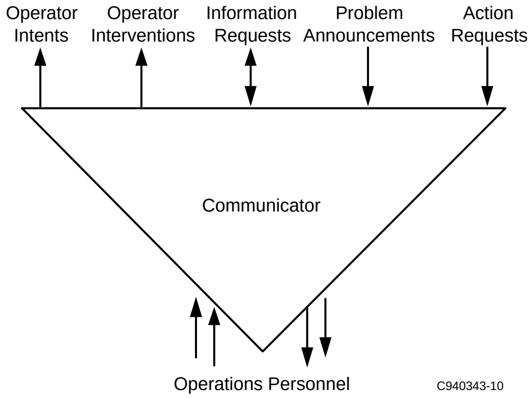
We anticipate that the bulk of the Monitor’s assessment and remediation activities will not occur in real time. Instead, the Monitor does its work off line, and remediation recommendations are provided when the Monitor has sufficient cause.

How it Interacts with Other Roles. The Monitor “reads” messages passed back and forth between all of the AEGIS modules. It interacts with the Communicator to notify users of detected problems and remedial actions, and with the Knowledge Customization Toolkit to facilitate the acquisition of new knowledge and the appropriate incorporation of that knowledge into AEGIS. It provides automatic feedback to those other Roles capable of accepting it. Operations team members are able to:

- View system self-evaluation of overall and individual Role performance.
- Enter user evaluations of AEGIS actions to improve future performance.

The Communicator Role

What it Does. Each of the AEGIS Roles needs to interact with users at various times. Moreover, they are all running simultaneously. To give each a separate interface would lead to confusion. The Communicator module provides a common user interface to AEGIS. It also serves to isolate the modules from the details of particular display and communications hardware that may vary from one installation to another.



The Communicator manages interface devices to make the best use of users' attention. Messages arrive asynchronously from other modules; some may be much more critical than others. The Communicator brings the critical items to the attention of the appropriate users. For example, if the next planned action demands an operator adjustment to a rarely used valve, the Communicator can summon the controls for that valve instantly. Each member of the operations team can quickly receive information on plant state, goals, and context-appropriate actions that are pertinent to their activities, improving speed of response and eliminating sources of human error.

How it Helps. Poor access and presentation of information has been identified as a serious bottleneck in abnormal situations. Both problems are addressed by the Communicator role. Because AEGIS is always aware of the current state of the plant and the immediate plans for control, presentations and access to displays can be made context-sensitive. The Communicator is aware of the operator's information load and capabilities, and the amount of information on a given display surface can be regulated to avoid confusion and excessive workload, such as the flood of alarms described in the earlier steam plant operations scenario.

Communications problems are another major contributing factor in abnormal situations. The issue is often the speed and accuracy of information transfer. The increased noise level in the control room, from reaching key personnel and handling low-priority radio traffic, makes conversations difficult. In addition, finding out who to call and how to reach them adds valuable time to performing interventions. The Communicator can improve this situation by automating some of the message transmission tasks.

How it Works. The Communicator makes use of existing, human-computer interface devices by deciding when and where information is needed to best support operator tasks and then presenting that information in the best format available. The Communicator makes use of familiar formats (e.g., those available in the DCS environment) whenever possible, and makes use of novel formats via existing equipment (e.g., novel plan scheduling screens, vocal instructions, or advice via telephone).

The Communicator also keeps track of the users' current active interface devices. The Communicator uses this information to route appropriate information to the relevant devices. In some cases, those devices might be radios or telephones; the Communicator generates or forwards voice messages as needed. For example, it knows that Jane Smith is the current field operator, that she was last sent to Holding Tank 81, and that her radio monitors channel D. An emergency near Tank 81 may trigger AEGIS to plan special actions for all field operatives in the area. The actions are passed to the Communicator, which radios the message to Jane Smith on channel D.

How it Interacts with Other Roles. The other modules forward their user interaction needs to the Communicator. The Communicator selects among information available and transactions requested according to priorities, resources, and preferences of the individual human operator in his or her current context (equipment available, ongoing goals and plans, concurrent activities and workload, etc.). Requests for information to be displayed or collected are addressed to individuals serving a given job function. The Communicator knows who those people are and keeps track of where they can be reached at any time. Some of the modules may keep open channels with the Communicator so that users can provide unsolicited information and commands to AEGIS.

If the Communicator is unable to complete a transaction within the allotted time, it signals a problem to the Monitor. User intent information is sent to the Planner and Goal Setter. The users may request desired information directly via the Communicator, which may in turn need to post these information requests to the State Estimator (or other Roles) in order to comply.

Key Technical Challenges to Delivering Effective Solutions

All operations personnel must have better decision support from the DCS if abnormal situations are to be efficiently and effectively managed. The AEGIS collaborative decision support solution requires that technical challenges be overcome in three strategic areas:

- **Human-machine interaction—**A comprehensive approach to the design of the human-machine system interaction is needed so that a single user interface environment provides operations personnel with information appropriate to their needs, while at the same time supporting the collaboration of appropriate members of the operations staff in solving the problem as a team.
- **System architecture—**To provide accurate, timely support in abnormal situations, a system architecture is needed that supports multiple processing modules, data bases and knowledge bases. These various software modules must communicate their conclusions with each other in real time and must remain coordinated among themselves and with human operators. Many past efforts have failed because this problem alone is so challenging.

- **System customization**—A major practical challenge in collaborative decision support technologies is configuring their capabilities to the idiosyncratic and dynamic nature of the plant processes and operations. Aspects of the software modules need to be customized with specific knowledge about the operations, equipment, personnel, and procedures of a specific site. Acceptable solutions need to be self-adaptive or easily customized by plant personnel.

Collaborative Human-Machine Interactions

AEGIS's functions are distributed over a set of six modular roles as described in the AEGIS vision. These specific roles were identified to provide operations assistance in those critical areas where recurrent behaviors occur in ASM practices (Reason, 1986, Cochran and Nimmo, 1997). Collectively, these modules provide automated assistance for the human activities of Orienting, Evaluating, and Acting, along with a mechanism for communication with plant personnel and a mechanism for modifying and improving AEGIS behavior. The AEGIS concept emphasizes human-system *collaborative* interaction; thus AEGIS will continuously interact with the plant operations team by configuring information as appropriate for the task of individual human users to facilitate the coordination of their operations. AEGIS will allocate tasks between people and computers based on the strengths of each. For example, AEGIS will improve Orienting by summarizing large amounts of data, Evaluating by resolving complex problems under pressure and formulating schedules, and Acting by managing or replacing human actions in time-critical situations. The development of AEGIS will restructure the ASM tasks to use the strengths of the computer (automated data analysis, rapid computation, etc.) to augment the strengths of plant personnel (flexibility, creativity, common sense). An important aspect of our technical approach is to recognize that ASM is an integrated activity. Hence, we have developed a user interface framework that provides the operations team a single window on operations, a task-centric layout of views, and mixed-initiative approach to human-machine interactions.

Single Window on Operations. The demands of process control, and in particular the need to interact with hundreds of instruments without adverse impact on the operators' awareness of the overall state of the plant, led the designers of distributed control systems to develop the "single window to the process" concept. In the AEGIS program, this concept has been extended to include all computer-based interactions supporting operations team members' ASM activities. This functionality includes access to current DCS operating display functionality, interactions with AEGIS diagnostic and decision support applications, logbooks, plant procedures, and other plant documentation. This design principle requires us to ensure that all interaction with the process take place in a unified, consistent, and comprehensive user interface. As new capabilities are added to the process control system and AEGIS components, they are required to be integrated into the existing user interface environment.

Task-Centric Layout. The AEGIS view library provides a suite of display views that comprise a set of information and interaction objects that covers the range of normal and abnormal situation management activities. Together, the suite provides a task centric structure for organizing custom graphic views. Based on an analysis of the kinds of activities operators engage in for both normal and abnormal operations, we defined a set of view types to support activity clusters (See Table 1 for brief description of each task view.

Mixed Initiative Interactions. For a variety of reasons, many decision support systems have been criticized for being to brittle as well increasing the possiblity of human error (Smith, Guerlain, Smith & Denning, 1996). Consequently, we have taken a mixed initiative approach to the design of interactions with AEGIS components to enable a more collaborative human-machine interaction. The mixed initiative functionality enables the users to influence the behavior of the machine, and at the same time, the machine can influence the behavior of the user. For example, in the traditional alarm notification systems, the engineers preconfigure the system to detect a set of process conditions in which the operator needs to be alerted because some important action is required to prevent the occurrence of undesirable situation. The condition under which the machine sends a notification to the user is fairly static. Moreover, it is difficult to accurately anticipate all situational needs for notifications. This makes the preconfiguration model less than adequate for ASM. In practice, operators may get too many notifications or too few for a given plant situation. In reality, the conditions under which notifications are needed are quite dynamic. Users need the ability to tell the notification systems what conditions are important at for the current situation and intervention tasks. Hence, we have created a mixed initiative approach. Where the user can take initiative to define a notification object to help them perform a particular task. Moreover, the AEGIS system can determine a need for a notification and create a new notification monitor.

Table 1. Set of Task Views designed to support Operator Interactions with DCS, AEGIS, and Plant Information Systems.

View Type	View Description
Status	Operators get a summary view of the status of plant processes that enables orientation to the location and priority of disturbances and unexpected process behaviors. This view spans the scope of control of a single operator as well as the process units immediately upstream and downstream.
Operation	Operators access a broad range of functionality in a single display that is the equivalent functionality found in today's schematic, group and detail displays. The equivalent of a hierarchy of views on the plant exist in a single display with different kinds of information and interactions emphasized at each level.
Diagnosis	Operators can diagnose the cause and impacts of disturbances indicated in the Status and Operations Task Windows. With the advent of diagnostic applications and smart devices that can assist the operator in diagnosing abnormal conditions, this view allows the user to see the evidence associated with diagnostic and alarm notifications, evaluate and rank the highest priority threats (disturbances), and identify the source of threats in terms of root causes.
Notification	This display integrates the current process alarm notification events (found in current DCS alarm summary displays) with other types of notification events supporting diagnostic, decision support and collaborative team communications.
Trends	This process monitoring view allows the user to configure a set of real-time trends to proactively assess status and behavior of the plant. Although, trends are available in other task windows, the trend functionality is tailored to the specific kinds of activity supported in those windows.
Decision Support	Operators can evaluate the significance of current threats to operational goals, establish plans to respond to imminent or current abnormal conditions and track progress in executing intervention activities.
Logs	Operations team members record and browse significant plant changes or activities. Moreover, this log reporting system is integrated with an incident/near-miss reporting system.
Documents	In addition, operators dynamically assemble information through access to the myriad of documents in the plant information systems. These documents include drawings, equipment specifications, procedures, incident reports and operating instructions.

System Architecture

A key innovation of AEGIS is a system architecture that supports the collaboration of a set of independent diagnostic, planning, and operator support applications. Previous approaches to solving this problem have attempted to build comprehensive, monolithic applications, which inevitably have become large and difficult to maintain. AEGIS, on the other hand, is designed to permit a variety of specialized applications to work together to identify problems and aid in their resolution. In this section, we describe to aspects of the architecture that address problems associated with previous monolithic approaches.

Nonmonolithic—Distributed, modular architecture. Each of the six AEGIS roles is implemented as a set of software application modules (See Figure 3). The AEGIS modules must be capable of distributed and partially independent action due to the variable nature of data flow and processing demands on each module. On the other hand, all modules must cooperate to produce effective overall behaviors—this requires communication of results and needs of information between the modules. In order to address these potentially conflicting needs, we developed the Plant Operations and Control Language (POCL) and instantiate it in a blackboard-like communications architecture which serves as a common area for exchanging messages and information posted there by each of the separate AEGIS modules.

These modular software applications work together to determine the current state of the plant, decide upon the most appropriate goals to pursue, develop plans for pursuing those goals, and for executing those plans and monitoring the execution process. In addition, applications are responsible for communicating with plant personnel and for monitoring AEGIS itself.

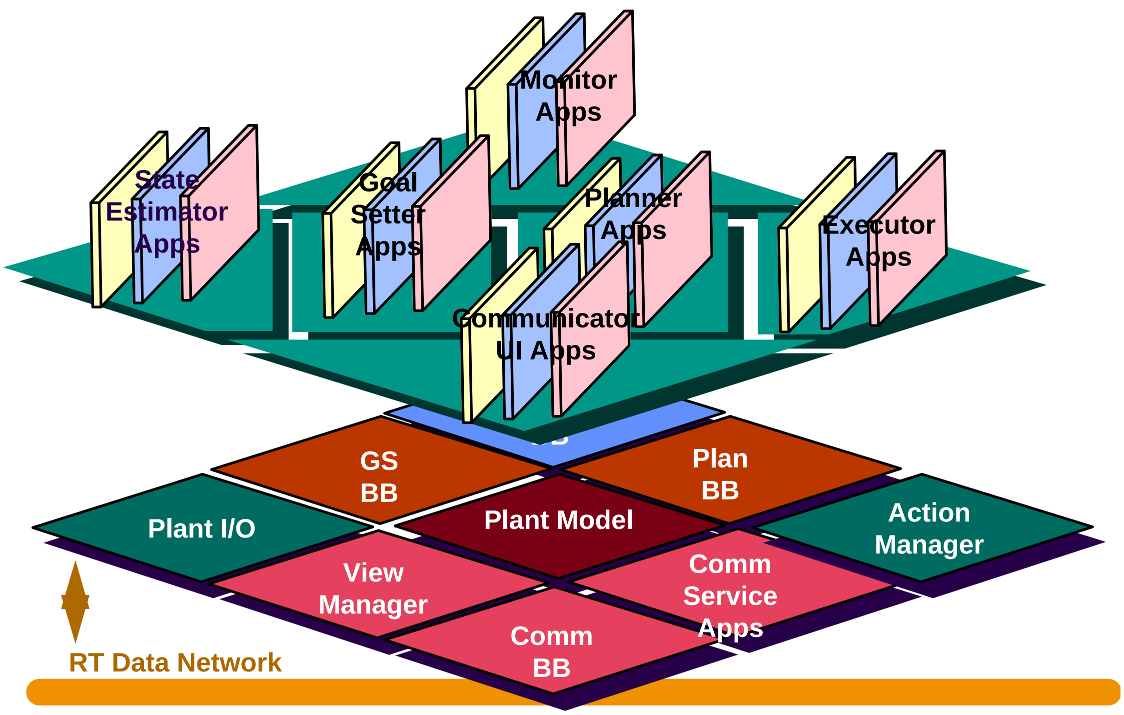


Figure 3. Distributed Modular Architecture with Multiple Component Applications for each of the Functional Roles

Extensible—Open API for Application Developers. The AEGIS prototype is being developed in a layered architecture based upon an open standard, and so will run on any DCS which supports that standard. The software consists of an infrastructure supporting many different kinds of applications, all sharing a common Plant Operations and Control Language (POCL) and a common blackboard on which messages in that language are shared.

The Plant Operations Communication Language (POCL) is built around human-level concepts in the operations domain to facilitate knowledge acquisition and later knowledge revision. The POCL specifies the major conceptual classes such as situations**,** *plans*, *goals*, *actions* as well as others. Each of these classes contains a hierarchical set of entities or objects that, in effect, comprise the common *vocabulary* by which AEGIS modules communicate with each other. The internal reasoning a module performs is in any format convenient for that module, but the module must express its conclusions and requests for information in the vocabulary of the POCL. Conclusions and requests are posted to a central blackboard or shared memory area, from which they can be accessed by all other modules. Specific messages posted to the blackboard by the various modules are generally concerned with the activation or deactivation of a specific conceptual entity (situation, goal, plan, or action) at some time and for some expected duration. For example, a message from the State Estimator might be: ACTIVATE SITUATION: VALVE-STUCK at TIME 20:14:53 with parameters 106 (the specific value referenced) and 76% (the point at which the valve is stuck). Figure 4 shows the operation of the POCL by illustrating the flow of information between AEGIS modules via a common message area, the *blackboard*.

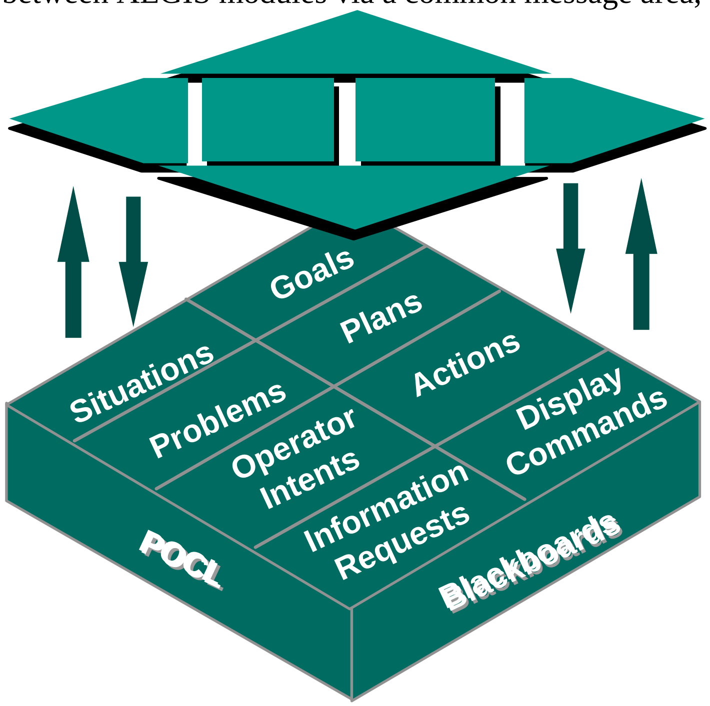


Figure 4. Information Flow between AEGIS Modules Using the Vocabulary of the Plant Operations Communication Language

There are only two general classes of alternatives to a POCL and blackboard approach to AEGIS system communications. The first is to construct a unified (non-distributed) AEGIS system that cycles through its modular functions, passing the results of one module (e.g., State Estimator) to the next module in line in a serial fashion. The problems with this approach are (1) the required delays while the system cycles through its modules (and coordinating incoming data from multiple sources during those cycles), and (2) the fact that the messages passed from one modular function to another must still be stipulated in some vocabulary in advance. The second alternative is to stipulate direct and dedicated message-passing protocols between each module without resorting to a blackboard (or similar) architecture. Although this approach still requires the creation of a vocabulary of acceptable messages, it does permit a more distributed or parallel processing approach that facilitates real-time operations.

While dedicated, direct message passing between AEGIS modules might be possible and might improve speed of system operations, we believe the modularity of the POCL and its blackboard architecture has advantages that outweigh these. Modularity in the POCL makes it easier to modify plant operating procedures, to revise or "grow" these procedures when equipment modifications are made, and to monitor and revise AEGIS operations via human assistance. For example, if a new set of diagnostic procedures improves the reliability of the State Estimator's performance, no changes need be made to AEGIS knowledge bases as long as the State Estimator can continue to communicate the same vocabulary of situations to the other AEGIS modules. If the improved diagnostic capability means that new plans, goals, and actions are now possible for ASM (or that new information is needed by operators), then only small, isolated portions of each AEGIS module's knowledge bases need to be changed to handle these new capabilities—and the hierarchical nature of the POCL facilitates the tracing of affected components. Finally, the fact that the entire representation is closely tied to human operators' concepts of plant operations serves to make the capture of new knowledge straightforward.

Customization Tools

One of the challenges in making AEGIS a cost-effective addition to future control systems is to minimize the effort needed to customize the AEGIS component applications to the specifics of a given plant. In future phases of the program, we will develop these customization tools. One promising approach is to develop a single model of the plant that can be shared with the all AEGIS roles and the DCS. This model contains generic plant equipment descriptions that can be tailored to the specifics of a given plant. Another element of a tools solution will be to provide tools to rapidly exploit existing plant information containing process flow diagrams, plant piping and instrumentation diagrams, and operating procedures.

Summary of AEGIS Development Progress

In Phase I of the program (completed March, 1996), the first AEGIS prototype was developed which comprised the software infrastructure of AEGIS, a suite of State Estimation applications, and early prototypes of the AEGIS console operator's interface. The prototype was linked to a simulated refinery unit and tested on a variety of induced problems. AEGIS was able to consistently identify the problems to which it was exposed, and the AEGIS architecture was qualified for further development in Phase II of the program.

In Phase II (completed March, 1997), the functionality of the AEGIS prototype was significantly enhanced to incorporate a more comprehensive process model and a more advanced prototype of the AEGIS console operator's interface. The new interface was designed for operations during normal and abnormal situations, and included a consistent user interface model and comprehensive support for notifications, navigation, diagnosis, and monitoring. The process model was expanded to incorporate a Vapor Recovery Unit (VRU) in addition to the FCCU modeled in Phase I; the model's complexity has increased by more than a factor of two. The scope of knowledge of AEGIS was expanded to include over 700 items of equipment in the process simulation, over 400 operational goals, and over 4500 possible malfunctions. AEGIS was able to consistently identify the problems to which it was exposed, and present a coordinated view of the problem to the operator. The AEGIS architecture was qualified for further development in Phase III of the program, which will focus on refining the operator interface applications and developing methods of collaboratively generating, executing, and monitoring recovery plans.

AEGIS has been designed as a very modular, very distributed system, intended for use in an open, multi-vendor environment. The core of the second AEGIS prototype consisted of infrastructure for providing system services, acquiring process data, and providing blackboards for inter-application transactions. A suite of state estimation applications employing a variety of sensor validation and process diagnosis technologies (including knowledge-based systems, sign-directed graphs, and quantitative and qualitative methods) worked to identify problems in the simulated process. A suite of communication applications worked to present process data to the console operator. These applications, collectively called the Communicator, presented a view of the process that is sensitive to the operator's workload, the process conditions, and the operator's current knowledge. The Communicator integrated functions required for understanding and responding to process upsets with those required for monitoring and controlling the process during normal operations. The Communicator also provided assistance to the operator in diagnosing process problems. The prototype was implemented using Gensym's G2, C and C++, Perl, Microsoft's Visual Basic, Java, and a few other specialized applications and languages.

The AEGIS testbed now consists of:

- two simulated refinery units (FCCU and VRU),
- a Honeywell TDC3000 Distributed Control System,
- a variety of networked workstations (UNIX and Windows NT OSs) running 25 component applications that comprise AEGIS itself,
- a prototype operator console, and
- a variety of supporting hardware and software.

The simulated refinery unit consists of a Fluid Catalytic Cracking Unit (FCCU) and its associated fractionator, feed and air heaters and blowers, waste heat boiler, and compressors as well as a Vapor Recovery Unit consisting of five towers and associated heat exchangers, pumps, reboilers, and other equipment. The simulation has been constructed by combining and extending first-principles simulations used in Honeywell Hi-Spec Solutions' SACDA Trainer. It provides real time data about, and access to, over 450 sensors and actuators. The simulation runs on a DEC Alpha, and is accessed by the TDC via a dedicated network link.

The TDC provides for traditional DCS control capability for the simulated FCCU, including a user station providing schematic, group, point, and alarm displays of the unit, and regulatory, supervisory, and advanced control algorithms for the unit itself.

The AEGIS prototype runs on a variety of Sun , HP, and Pentium hardware using Solaris, HP-UX, and Windows NT operating systems. AEGIS acquires its data via a link to an AxM module on the TDC 3000, and displays its conclusions via an operator's console consisting of several networked Windows NT and Honeywell GUS systems connected to 21-inch monitors equipped with touchscreens, as well as a 40" Seufert Systems Overview display.

The first AEGIS prototype was formally evaluated in 22 scenarios including sudden and unexpected malfunctions, problems that developed over the course of an hour, and problems originating in process equipment, process control devices, and the process itself. Fast upsets involved a deviation of a process parameter of up to 15% of range over a one minute period; slow upsets took 60 minutes to reach the same level of deviation. In all of the test scenarios, the AEGIS prototype was able to take advantage of the diverse strengths of its variety of state estimators to consistently identify the broad variety of problems that were presented. Moreover, AEGIS was able to identify the slowly developing problems well before they became significant (on average before drifts reached 5% of scale).

The second AEGIS prototype is currently being evaluated by operations personnel from Consortium Member companies. The evaluation protocol aims to assess the usability of the AEGIS Communicator, and to empirically determine whether operators using AEGIS are more capable in responding to a variety of process upsets than operators using current control systems technology.

A key feature of AEGIS is an architecture that supports the collaboration of a large number of independent diagnostic, planning, and operator support applications, all working together to solve the problem and keep the operator in control. In Phase I, this approach permitted AEGIS to combine diagnostic approaches which are powerful in some areas but less so in others to enable an overall diagnostic ability that is more accurate than any single application could be. In Phase II, we extended this approach to user interface functions, permitting specialized user interface applications to work together to present the operator with information that would otherwise have to be laboriously extracted from multiple independent sources. This architecture will ultimately support the interaction of process operators with each other, with field operators, and with other plant personnel.

AEGIS has been developed using an open architecture so that state estimators, user interface applications, and ultimately planning, modeling, documentation, and data management applications can be developed and incorporated by Honeywell, Consortium members, and independent parties. The current prototype was designed and developed by user interface specialists, process engineers, and software engineers from the Honeywell Technology Center, Honeywell Industrial Automation and Control, and Honeywell Hi-Spec Solutions, with significant assistance from Amoco, Exxon Gensym, and Texaco.

Issues remain to be addressed in several areas, and work will continue in Phase III: State estimators need to be refined; tools for easy installation and application of AEGIS Roles need to be developed; User interface functionality needs to be extended and enhanced; and the entire realm of planning and response needs to be integrated.

The ASM Consortium remains committed to this effort, and believes that its continued investment and that of the NIST Advanced Technology Program will ultimately lead to a solution resulting in a reduction in the costs of petroleum processing and chemical manufacturing and a significant benefit for U.S. economic growth.

References

Cochran, E. and Nimmo, I. (1997). Managing abnormal situations in the process industries I: automation, people, culture. *Proceedings of the MVMT Workshop*, Ann Arbor MI.

Nimmo, I. (1995) Abnormal situation management. *Process and Control Engineering*, **49**, 5, 8, November, 1995.

Nimmo, I. and Cochran, E. (1997). The future of supervisory control systems in the process industries: Lessons for discrete manufacturing. *Proceedings of the MVMT Workshop*, Ann Arbor MI.

Reason, J. (1986). Recurrent errors in process environments: Some implications for the design of intelligent decision support systems. In E. Hollnagel (Ed.), *Intelligent Decision Support in Process Environments*, Berlin: Springer-Verlag.

Smith, P.J., Guerlain, S., Smith, J.W., Denning, R. McCoy, C.E., and Layton, C.F. (1996). Theory and practice of human-machine interfaces. ???