AN INTEGRATED APPROACH FOR INTEGRATED INTELLIGENT INSTRUMENTATION AND CONTROL SYSTEM(I^3CS)

C. H. JUNG, J. T. KIM, K. C. KWON
Korea Atomic Energy Research Institute
Yusong, Taejon, Republic of Korea

Abstract

Nuclear power plants to guarantee the safety of public should be designed to reduce the operator intervention resulting in operating human errors, identify the process states in transients, and aid to make a decision of their tasks and guide operator actions. For the sake of this purpose, MMIS(Man-Machine Interface System) in NPPs should be the integrated top-down approach tightly focused on the function-based task analysis including an advanced digital technology, an operator support function, and so on. The advanced I&C research team in KAERI has embarked on developing an Integrated Intelligent Instrumentation and Control System(I^3CS) for Korea's next generation nuclear power plants. I^3CS bases the integrated top-down approach on the function-based task analysis, modern digital technology, standardization and simplification, availability and reliability, and protection of investment.

1. INTRODUCTION

All of the nuclear power plants in Korea are operating with analog instrumentation and control(I&C) equipment that are increasingly faced with frequent troubles, obsolescence and high maintenance expense. Electronic and computer technology have improved rapidly in recent years and have been applied to other industries. The digital technology provides advantages such as processing of numerous data, improvement of system reliability, flexibility of adding new functions, automation of periodic tests, self-diagnostics, and improved operation and maintenance using standardized components. So it is strongly recommended that we adopt the modern digital and the computer technology to improve plant safety and availability.

The TMI-II accident was primarily caused by a wrong identification of the plant state resulting from human factors deficiencies in the plant information system. It is very difficult for the operator to identify abnormalities of process state in transients. For the sake of identification of the abnormal conditions, the operator should get sufficient and credible information such that the operator diagnoses and prognoses the process states, and confirm operator's actions. It is a good approach that the integrated top-down approach tightly focuses on the function-based task analysis including an advanced digital technology, an operator support function and so on. Figure 1 illustrates the strategy for applying the integrated approach into NPPs in Korea.

In light of the need to improve MMIS of NPPs, the advanced I&C research team in KAERI has embarked on developing an **Integrated Intelligent Instrumentation and Control System(I^3CS)** for Korea's next generation nuclear power plants. I^3CS bases the integrated top-down approach on the function-based task analysis, modern digital technology, standardization and simplification, availability and reliability, and protection of investment. The initial effort in this multi-year project focuses on process monitoring, alarming, alarm diagnosis, increasing automation, human-performance evaluation of the developed system and a development of methodology of software verification and validation. We are developing Alarm and Diagnosis-Integrated Operator Support System, called ADIOS, to filter or suppress unnecessary or nuisance alarms and diagnose abnormality of the plant process. ADIOS has been built in an object-oriented AI environment of G2. To increase automatic level, ASICS is developed to automate low power level from cold shutdown to 5 % reactor power level by using supervisory modular control scheme. To evaluate and validate the performance of the developed system, a study is progressed on the field of human-performance evaluation and software verification and validation. [1-4]

2. TARGET OF I^{3}CS

To establish the technical goals of I^{3}CS, we have evaluated the technical level of I&C, such as Computerized Compact Workstation, Digital Control, Digital Protection, Operator Support, Network, and Digital Data Acquisition and Nuclear Integrated Monitoring Technique. The results of the evaluation were to increase the level of automation applying the advanced control techniques such as supervisory control and automatic startup/shutdown system, to consolidate the function of diagnosis and operator support in process transients, and to integrate these systems properly according to operator's cognitive mental model. Fig. 2 shows the technical goals of I^{3}CS.

We proposed I^{3}CS for beyond the next generation NPPs in Korea. I^{3}CS reflects a concept of EPRI Utility Requirement Document such as top-down approach based on the functional task analysis, modem digital technology, standardization and simplification, availability and reliability, and protection of investment, etc. To accomplish this purpose, the major targets of I^{3}CS were established with the following major elements.

Reduced Human Errors

First of all, to reduce human error, the integrated design methodology should be developed. There is a feasible way of the integrated top-down approach to reconstruct the I&C architecture including control room based on a task allocation by the functional-based task analysis. Second, a cause bringing about human error should be eliminated. Because the automatic start-up/shutdown system reduces the operator intervention in operation of start-up and shutdown mode, a mistake of operator will be significantly reduced. Intelligent operation support system aids to identify the plant state in the transient condition, make a decision of the operator tasks, and guide operator actions.

Improved Availability and Reliability

The reactor protection system and safety related system will be designed by digital technology with an automatic test function and self-diagnosis features. These technologies will significantly decrease the unnecessary reactor trips. The use of digital technology in NPPs takes advantages such as processing of numerous data, flexibility of adding a new function, and reduction of operation and maintenance expense. However, an application of digital technology may bring about a new problem to ensure safety and reliability as concerns common mode failure and software verification and validation(V&V). Especially because of the characteristics of software, the safety and reliability of software are critical issues in the digital I&C system of NPPs.

Standardization and Simplification

I^{3}CS uses the industrial open architecture and off-the-shelf equipment manufactured in the domestic industry. Because the off-the-shelf equipment is developed with the design of adapting the industry standard, modularizing and simplifying, repair of I&C equipment will be accomplished by simple modular replacement in the field. Operation and maintenance cost may be reduced.

Assure License

An application of digital technology, especially digital safety system may bring about the new problems such as common mode failure, software verification and validation(V&V), establishment of quality assurance program and resolution of elecro-magnetic interference. A number of method and tool to solve these problems are being studied and developed, but not completely resolved. These problems are directly connected with licensing issues. For the sake of protection of utility's investment, license should be assured by solving these problems.

3. INTEGRATED APPROACH

It is expected that I&C systems, particularly the control room, for future plants will be strongly focused on human factors engineering. Therefore, the design of I&C architecture and the control room should be done in terms of operator tasks for human error reduction. The design concept that provides the greatest consideration to the operator is only achieved by the integrated approach to reconstruct the whole I&C structure and control room based on the allocation of functional task-centered human operator. MMIS of next generation NPPs in Korea integrates the operator support functions, the process operation functions and the monitoring functions according to operator's cognitive mental model.

The integrated top-down approach focused on operator tasks and should be performed on the basis of the previously obtained system design technology, the developed research results, and the transferred technology from ABB-CE. In the development stage, we will develop a standard design package(I^3CS) of the level. If there are some fields of technology lacking in Korea such as diagnosis model, operator response model, supervisory control techniques and performance evaluation, etc, they will be provided by cooperation with foreign suppliers.

4. APPROACH FOR I^3CS

The I^3CS consists of three major parts; (1) the advanced compact workstation, (2) the distributed digital control and protection system, including Automatic Startup/shutdown Intelligent Control System(ASICS), and the computer-based alarm processing and operator support system, called Diagnosis, Response, and operator Aid Management System (DREAMS). The advanced compact workstation adapts a control workstation concept by adding the new design features such as supervisory functions, operator support display, and selected mobile overview display, etc. The distributed digital control and protection system are designed by using the robust and fault-tolerant control method, the intelligent supervisory control technique, the automatic startup/shutdown system, the data communication network, etc. DREAMS provides the operator exact information by using the dynamic alarm processing techniques, the model-based fault detection and the diagnosis functions, etc.

4.1. Advanced compact workstation

The advanced control workstation has adapted a computer-based compact workstation concept on the application for next generation NPPs. By the first effort to allocate the function of the computer-based compact workstation, the function-based task analysis was performed. This advanced compact workstation is upgraded by adding the new design features on the basis of functional-based task allocation. The added design features are as follows:

- extension of supervisory functions;
- extension of coordinated function between operators;
- consolidation of operator support function;
- Intelligent soft control technique;
- electronic display of normal and emergency procedures;
- Extension of overview display;
  - two detailed system overview mimic displays;
  - a selected movable overview display.

4.2. Fully distributed digital control and protection system

Through the function-based task analysis, the control and protection system is also adapted in I^3CS by adding the following design features:

- Fully using data communication network.
- Supervisory control coordinating primary and secondary system.
- Automatic startup/shutdown system with supervisory coordinator.
- Robust and fault-tolerant control.
- Addition of Macro control functions.
- Certain resolution for common-mode failure, software V&V and EMI.

The first effort in the control and protection system is to develop the digitized system. The digitalization, especially of the protection system, has some problem such as common-mode failure, software verification and validation, and hardware electro-magnetic interference, etc. To solve these problems, the control system is duplicated using the different hardware and software, and the protection system adds the system-based hardwired backup system. The methodology for resolution of the problems of software V&V and EMI is being studied.

The second effort is to increase the level of automation. The increase of automation reduces operator intervention that is a cause of human errors. The automatic startup/shutdown system is developed for these purposes.

4.3. Automatic startup/shutdown intelligent control system (ASICS)

The target of ASICS automates operation from cold shutdown to 5 % of reactor power. ASICS uses hierarchical modular control scheme and supervisory control scheme. ASCIS divides the control scheme into three hierarchical control level. Fig. 3 shows ASICS's hierarchical control configuration scheme. In the first supervisory control level, supervisory coordinator confirms an action of the lower level controllers, supervises the plant state and coordinates the lower level controllers. The control level of the second operating mode divides the four control mode such as heating mode I sequence control, heating mode II sequence control, critical mode sequence control, and 2nd mode sequence control. In this control level, the mode sequential controllers controls the needed components of the lower level control system in each control mode according to the sequential procedure. As there are the break points between modes, the supervisory coordinator automatically checks and alarms a safe condition of control process and coordinates the lower level controllers. The major control in heating mode I is temperature control in the primary system. The major control in heating mode II is pressure and temperature control in the primary system. The major control in critical mode is reactivity control in Core. The major control in 2nd mode is level and pressure control in secondary system. The low control level is the same of the conventional control scheme.

4.4. Diagnosis, response and operation management system (dreams)

There are the strongly developing areas. At present, one of the most important issues in human factors engineering field is to reduce human errors. To reduce human errors, there are two ways that eliminate the essential cause of human errors by intervening operator and informing the operator what to precisely identify plant state in emergency condition and by directing the operator actions. DREAMS provides the operator an exact information that supports the operator to diagnose abnormalities of plant, to manage the operator response on the application of the following technologies:

- Computer-based dynamic alarm processing techniques:
  - alarm suppression on operating mode;
  - alarm suppression on direct precursor and cause-consequence relationship;
  - dynamic prioritization dependent on plant state.
- Model-based fault detection and diagnosis functions.
- Integrated operation support and management system with computer-based guide display of normal and emergency operation, and technical specifications monitoring.

The initial effort as a part of developing DREAMS focuses on intelligent process monitoring, alarming and diagnosis, namely Alarm and Diagnosis-Integrated Operator Support System (ADIOS). We are currently focusing on implementing an advanced alarm processing using G2 real-time expert environment. ADIOS uses equipment-state dependency, plant mode dependency, alarm generation, and cause-consequence relationship(sometimes called, direct precursor), and multi-setpoint relationship(sometimes called, level precursor), in addition to some unique methods. Our unique methods include separation of the process alarms (e.g., temperature or pressure alarms of the main process) from equipment-related alarms (e.g., vibration or lubrication alarms of a pump), presentation of status alarms (e.g., PORV not closed) on the process mimic, representation of group alarms assimilating information from several related alarms. Fig. 4 shows how the alarms are processed and presented in ADIOS.

Two different scales of ADIOS are under development using G2 real-time expert system shell; (1) a small scale with about 40 alarms to devise a generic architecture for alarm processing and presentation and also to demonstrate the basic concepts of annunciation improvement, and (2) a large scale with hundreds of alarms to show the alarm management in a more practical environment. The small-scale system is used as an example to illustrate the major concepts. Fig. 5 shows the process overview mimic display in ADIOS. Once the large-scale ADIOS is developed, it also shall undergo several performance tests including: (1) a preliminary test with the CNS, (2) verification and validation (V&V) of the ADIOS knowledge base using an automated V&V tool, called COKEP (Checker Of Knowledge base using Extended Petri net), and (3) a human-factors test using the Simulation Analyzer with a Cognitive Operator Model (SACOM) in the KAERI's Integrated Test Facility (ITF).

The activated alarms are then prioritized using several alarms processing methods, such as plant-mode dependency, equipment-state dependency, multi-setpoint relationship (i.e., level precursor), cause-consequence relationship (i.e., direct precursor), and so on. Each alarm in ADIOS is initially classified into one of two different priority groups: (1) the first priority group of priority 1 or 2, and (2) the second priority group of priority 2 or 3. This classification of every alarm is based on its importance as to the promptness of the operators' response needed, or the effect of the alarm on the plant process or equipment. The prioritized alarms are displayed on the process overview mimic, and also the chronological list of alarms is givens on another dedicated CRT, with those alarms categorized by systems shown on the third CRT as a spatially dedicated soft alarm panel. Priority 1, 2, or 3 alarms are shown differently in red, yellow, or white, respectively. The same color coding is applied to the alarm texts in the alarm list, and also to the window tiles on the soft alarm panel.

4.5. Safety software verification and validation (SSVV)

The use of computers in safety-critical, real-time, instrumentation and control applications requires that the issues of system performance, software verification and validation (V&V), software safety, and software related common mode failures be addressed. Resolution of these issues as they pertain to nuclear facility applications is an emerging technology. Nevertheless, for commercial nuclear applications, these issues must be adequately addressed during licensing process. The modern and KNGR designs in Korea will utilize computers in safety-critical, real-time I&C applications.

SSVV team is responsible for developing an indigenous technical capability for verifying and validating the software safety of computer-based I&C systems for safety-critical applications in nuclear facilities. The missions of SSVV team in KAERI are (1) to evaluate the worldwide issues of digital safety system in nuclear power plant, (2) to construct the high-assurance software development environment, (3) to develop the methodology to design and to V&V software important to safety, (4) to study the basic technologies on safety-critical software. We are conducting these missions successfully through the cooperative R&D with industry and universities, the globalization of R&D, and the collaboration with the regulatory body and the international standards organizations. Fig. 6 depicts the technological tree of SSVV and the relations.

5. CONCLUSIONS

In light of the need to improve MMIS of NPPs, KAERI has embarked on developing an Integrated Intelligent Instrumentation and Control System(I^{3}CS) for Korea's next generation nuclear power plants. I^{3}CS bases the integrated top-down approach on the function-based task analysis, modern digital technology, standardization and simplification, availability and reliability, and protection of investment.

The initial effort in this multi-year project focuses on process monitoring, alarming, alarm diagnosis, increasing automation, human-performance evaluation of the developed system and a development of methodology of software verification and validation. We are developing Alarm and Diagnosis-Integrated Operator Support System, called ADIOS, to filter or suppress unnecessary or nuisance alarms and diagnose abnormality of the plant process. ADIOS has been built in an object-oriented AI environment of G2. To increase automatic level, ASICS is developed to automate low power level from cold shutdown to 5 % reactor power level by using supervisory modular control scheme. To evaluate and validate the performance of the developed system, a study is progressed on the field of human-performance evaluation and software verification and validation.

REFERENCES

[1] KIM, J.T., HAM, C.S., KWON, K.C., LEE, D.Y., "The Strategy for the Advanced I&C System (I^3CS) Development", Proceedings of a Specialists' Meeting Organized by the IAEA in Co-operation with ISTec and held in Garching, Germany, 4-7 July (1995).

[2] KIM, I.S., HWANG, I.K., LEE, D.Y., PARK, J.C., HAM, C.S., "An Integrated Approach to Alarm processing", The 2nd American Nuclear Society Topical Meeting on Nuclear Power Plant on Nuclear Power Plant Instrumentation, Control, and Human-Machine Interface Technology, University Park, Pennsylvania, USA, May 6-9 (1996).

[3] Na, N.J., Kim, I.S., Kim, J.T., Hwang, I.K., Lee, D.Y., and Ham, C.S., "AI-Based Alarm Processing for a Nuclear Power Plant," FLINS'96, The 2nd International FLINS Workshop on Intelligent Systems and Soft Computing for Nuclear Science and Industry, Mol, Belgium, September 25-27 (1996).

[4] JUNG, C.H., " A Development of Automatic Control Modes for the Startup Operation of NPP," Proceeding of the Korean Nuclear Society Autumn Meeting, Vol. 1, Seoul, Korea (1995).

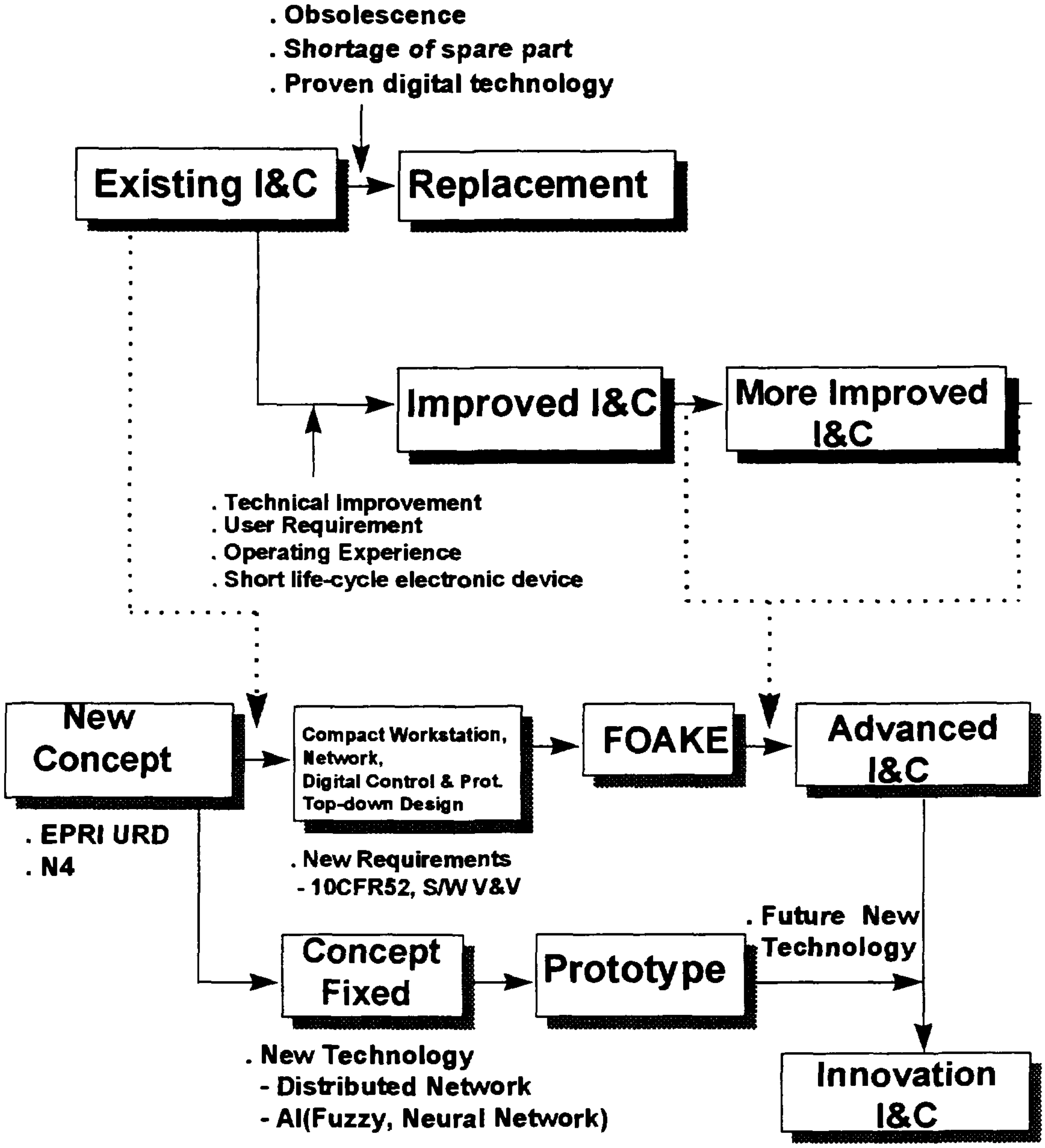

FIG. 1. The strategy for applying the integrated approach.

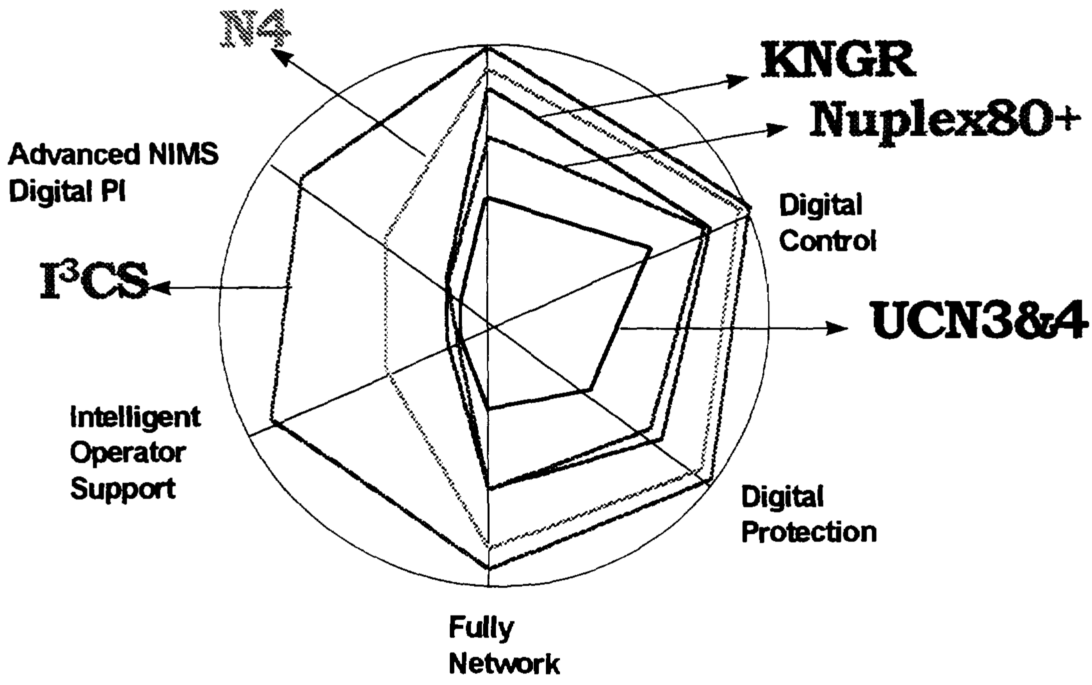

FIG. 2. The technical goals of I³CS.

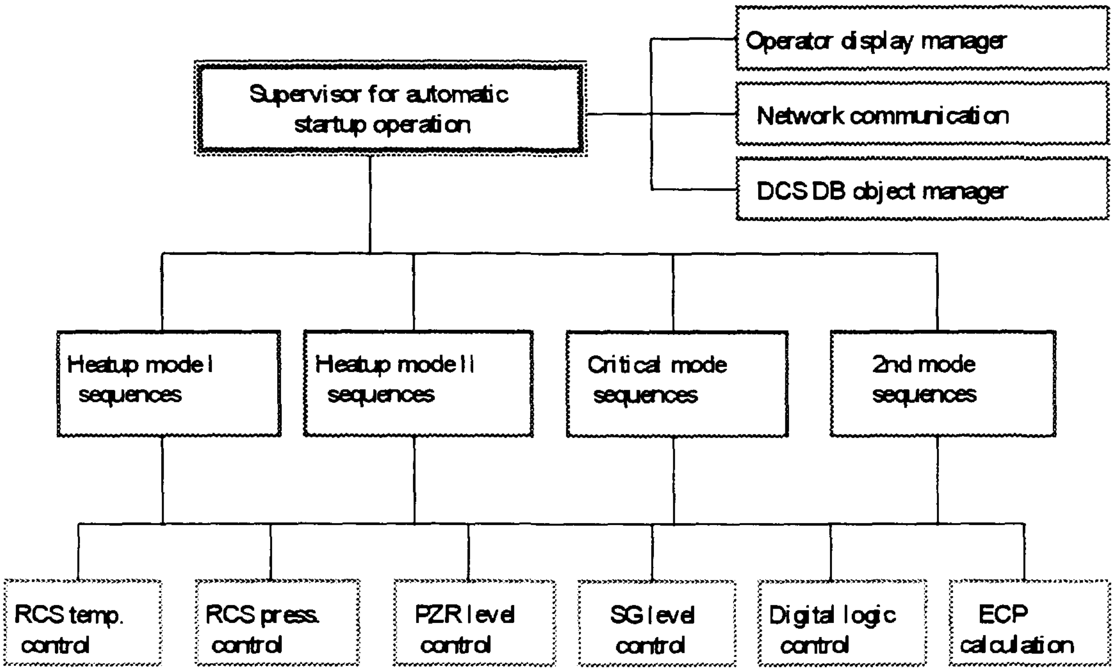

FIG. 3. ASICS's hierarchical control scheme.

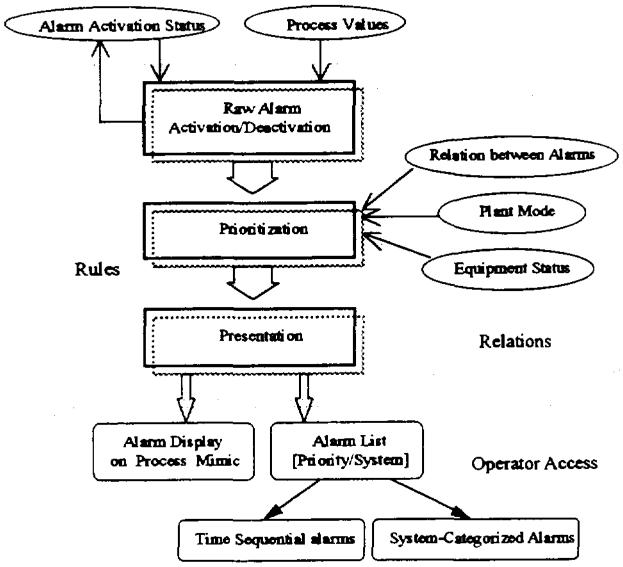

FIG. 4. Alarm processing flow in ADIOS.

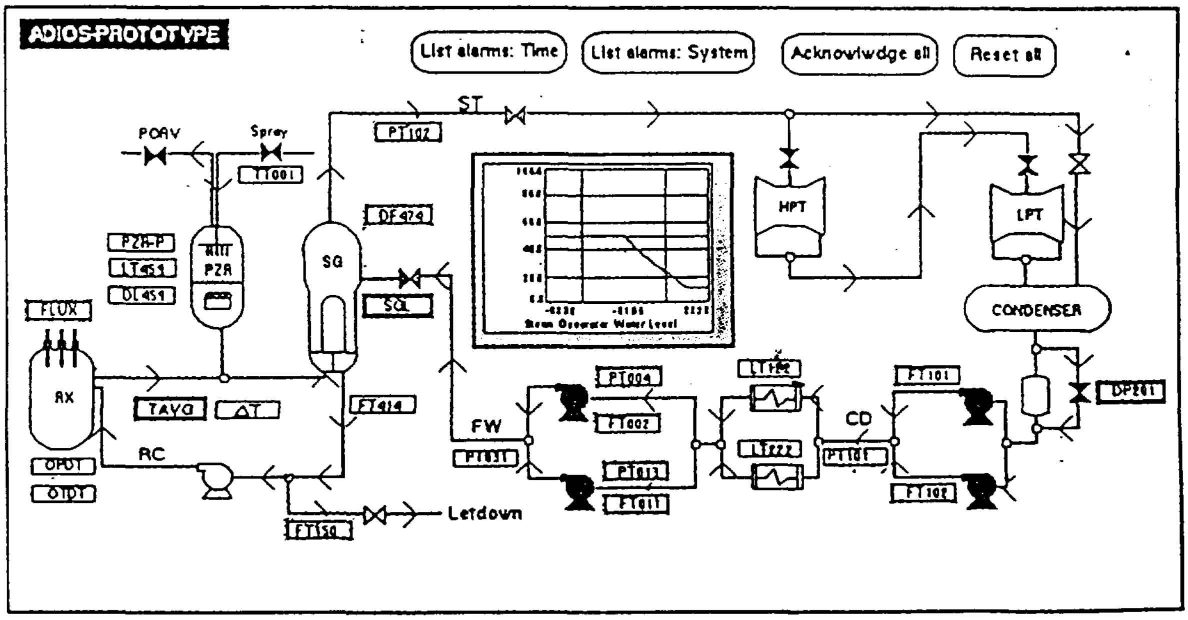

FIG. 5. Process overview mimic display in ADIOS.

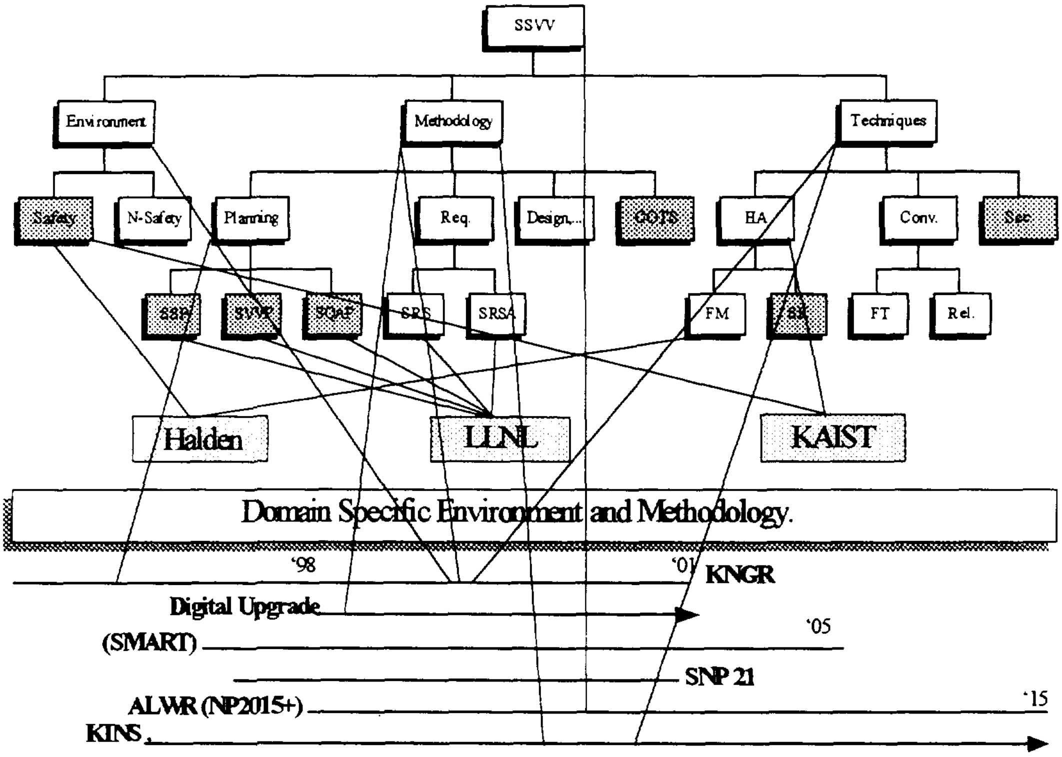

FIG. 6. Technology tree of SSVV and relations with others.