15th Triennial World Congress, Barcelona, Spain

# DESIGN CONCEPT OF AN INTERACTIVE INTERFACE FOR PLANT OPERATIONAL SAFETY

**Kensuke Kawai**

Toshiba Corp., Power Systems & Services Company,
Thermal Power Systems and Services Division
4-36-5, Tsurumi-Chuo, Tsurumi-ku, Yokohama-shi, 230-0051, Japan
Email: kensuke.kawai@toshiba.co.jp

Abstract: Some ethical aspects of automation system design are discussed, based on a case study in power plant automation. The discussion uses the "doing-good approach" and relates to three levels of design: business level, company level and engineering level. It is proposed that from the results of the case study that, in order to respect ethics in automation, the evolutionary design approach can strongly be recommended. *Copyright © 2002 IFAC.*

Keywords: Safety, Human-machine interface, Engineering ethics, Social impact of automation.

## 1. INTRODUCTION

When we discuss the ethical aspects of automation, it is proper to analyze the problems in three levels, which are corresponding to business level, company level, and engineering level.

The first level focuses on the relationship between business needs and system requirements. Here in this level, the effects of automation on the availability and type of employment will be reviewed. Any company should usually perform its business activity based on the business planning in mid-term. The automation philosophy shall be established in the context of the company's strategic planning. Especially, those in a infrastructure domain such as power, oil, or gas industry, should understand and have full access to the voice of the human operators in order to recognize the reality in the relevant plants.

Relationship between user engineers and the human operators in any company is defined as the second level, which focuses on the impacts of automation on the skill levels and job satisfaction of the human operators. In any automation system the human operator should learn the plant dynamics and operational expertise's throughout the interaction with the automation system. Operational philosophy in that sense is so important to be established inside the companies, which seek advanced automation as a part of the operation policy. User engineers and their counter parts of human operators must study the usability of the automation to be realized.

The third level focuses on the relationship between user engineers in a company and the system designers in another. In this level, the conflicts between user engineers and design engineers are to be solved across the enterprise. In order to achieve the human centered approach of automation design, it is quite appropriate to start asking "Who is the customer of this automation system?" It is rather difficult to identify and visualize the operational expertise to share it commonly. This transparency during both design stage and on-line stage is one of the most important features of successful automation. The final decision maker shall always be the human operator, even if the automation design might be highly advanced in nature.

In the following sections, the "doing-good approach" as an engineering ethics will be applied to realize the highly usable automation system in the field of power plant automation as a case study.

## 2. WHO IS THE CUSTOMER?

Automation design based on the voice of the human operators will be discussed in this paper.

In addition to a comprehensive automation system, which covers all the major operations during start-up to shut-down, including normal and emergency operations, there was a project to apply and develop the new control algorithm of optimum steam temperature control using auto regressive model and dynamic programming in a boiler process. The development project itself proved to be successful to bridge the gap between theory and practice in control and operation of fossil-fueled power generating plant.

During the commissioning of this project, however, there was an incident and its quick recover was needed in major plant equipment, which led to the formation of "Automation Review Committee" by the engineers both from the power company and plant/automation suppliers. Hardware modification to enhance the processing capability, which was needed to calculate the advanced algorithms on-line, resulted in one of the triggering events for the incident to happen.

During discussions after the plant disturbance, the final goal and objectives of the automation system, requirement definitions of human-machine interface, functions of the automation system, and the role of human operators were reviewed again to re-establish the real Voice of Human Operators.

Especially, how to give the necessary information at an appropriate timing to the human operator was one of the major design-review items of automation system. The messages given by the automation system shall be output serially, considering the human operators single-channel structure of information processing capability.

The clear distinction between automatic and demand message output during start-up and shutdown, were reviewed just from the beginning again. The result of the analysis and its revised automation design were applied to this project, which improved the usability by the human operator and the safety and reliability of the power generating plant.

Those aspects for engineering and maintenance, other than those of plant control and operation, were also analyzed to identify the management aspects of power generating plants, reviewing the voices of commissioning engineers, maintenance engineers and those of managers of the power company.

Although the voice of the human operators in the past might be analyzed from historical perspectives, it is quite interesting to note that the voice of future customers in control and instrumentation shall be fully understood, since the similar phenomena named "Innovator's Dilemma" had happened in this fields such architectural transfers as:

- from process computers to engineering workstations,
- from engineering workstations to personal computers,
- from real-time operating systems to UNIX operating systems, and
- from UNIX operating systems to Windows operating systems.

## 3. DEFINITION & FOCUS

Next, we will discuss the proper definition of a good automation system and its current practice.

The first steps to reach to the successful automation are to define the objectives of automation system, to determine the scope and depth of automation including automation modes available, and to introduce the patterns of regulating methods such as direct digital control, supervisory set point control and the like.

The goal of automation should never eliminate the human operator, but rather it shall establish the automation with autonomous nature, which means that the human operator welcomes the automation, or he or she has a positive attitude to use the automation interactively.

The objectives of automation system in Japan, were decided based on the social conditions of 1970s and 1980s. The scope and depth of automation were also subject to the technology level, then available. Starting from just a turbine run-up system, the automation system focused on the automatic operations during both start-up and shut-down of turbine and boiler, and it also focused on reduction of labor during normal operation, and restorative operations after plant emergencies such as FCB (Fast Cut Back) operation.

Although some important concepts were introduced, such as changeover between control mode/sequence-monitor mode, the matching of plant operational mode with schedule calculation parameters, and advanced features of improved human-machine interfaces, no overall measure was defined as a means of judging the appropriateness of the automation design, which corresponds to the objectives of automation. Very limited subjective evaluation was conducted as a usual practice, although there were few exceptions.

## 4. DESIGN TARGET & ANALYSIS

Analyzing the approaches of automation design will be described briefly as follows.

In our approaches to a successful automation design, the author and his colleagues needed in-depth analysis of a new concept of a Chain of triggers upon plant events. In this concept, automation knowledge can be described by state-space expression of N-inputs and 1-output combination. All the analog-type input could be treated as digital-type status by introducing the appropriate limit values to them. This means that we can treat in a consolidated way both the analog value with its limits and digital value now.

The next basic framework depends on the logical expressions by PANS (Pre-conditions)/CANS (Complete-conditions)/TANS (Timing conditions). This is a sort of production system, which specifies the knowledge of automation efficiently and effectively. In order to make this knowledge more understandable, packages of expressions were introduced, which defined plant master status (PMS), macro status determiner (MSD) of pre-conditions/complete-conditions, and the like.

Separation between the production rules and the procedural expression of feedback control was another consideration to accelerate the re-use of the automation knowledge from one project to the next. Visualization of automation logic and on-line real-time accessibility to it were also important features for the human operator, which intensifies the situation awareness of the status of the plants.

## 5. DETAILED DESIGN & IMPLEMENTATION

Detailed design and evolution of automation design is now the theme of this case study.

The automation design based on the experience over twenty five years is also coming to its close. As a variety of available technologies for this automation increases, automation design evolved into a better one to solve those problems encountered during commissioning and after the taking over of the power generating plants. Especially, human-machine functions were reviewed again and again to achieve the evolutionary improvement over the long period of design improvements. Although the very basic design concept were unchanged, this evolutionary approach enabled the introduction of advanced features of automation very safely and reliably.

The followings are some typical improvements in automation design:

- higher reliability of automation by duplicated system configuration,
- realization of duplication of CPU, shared memory, and controller backup,
- introduction of network architecture for distributed system configuration,
- introduction of operator-station concept, enabling all alarming and operation functions on a single client (Workstation/PC), and
- improvements of schedule calculation method, covering wider scope and depth of unit, as well as
- start-up operation and unit shutdown operation as a cycle.

The maintainability consideration was another aspects of successful automation. Not only the logic editor called Background processor used for the maintenance of production rules of automation logic, but the following maintenance functions were also made available during the last twenty five years of continuous improvement:

- maintenance function for data base and calculations,
- maintenance function for graphics and tables,
- maintenance functions for performance calculations,
- maintenance function for control procedures and operations, and
- maintenance function for commissioning.

## 6. SYSTEM EVALUATION

Finally as a case study, the overall evaluation in different cultures and countries is made.

As a part of final evaluation of the automation design, the basic design of this automation was applied to realize the plant automation in different cultures and countries, such as Australia, Canada, China, India, and Kuwait. Needs for flexibility of automation in these countries were not so strong compared with the case of Japanese utilities (where super-critical once-through boiler is used), since in these countries they introduced limited level of automation into the plant with sub-critical drum-type boiler.

In the next decade, gas-fired combined cycle plant will increase much more as a result of innovation in the field of power generation. Although the control of the gas turbine (GT) might be very complicated, they are carried out by a dedicated controller attached to GT. Other operations for HRSG (Heat Recovery Steam Generator) and BOP (Balance of Plant) as a part of comprehensive automatic operation are essentially simple, and the focus of the control and operation will be on the revolution in safety and security of human machine systems and the development in intelligent and critiquing systems for human operator assistance.

## 7. CONCLUSION

Responsibility as an engineer can be defined as an individual moral level or as a collective professional level. Since the automation systems in the infrastructure plants play the important role in a society, it is necessary and better be motivated for an engineer to do good to human operators, applying the transparent automation knowledge. It is not just to avoid or minimize plant operational risk, but it is highly recommended for an engineer, both of user company and designer's company, to try to do good, bringing in a highly USABLE automation system.

The problems concerning the design for operational safety by interactive interface is such a complex, moving-target issue that only the evolutionary design approach with initial design rules of automation is the possible option leading to the successful automation. Operational assistance in an adaptive way and deskiling mitigation of the human operators are also the indispensable part of practical automation. Starting from the identified design rules lead to the true modularity design of safe automation system.