Upgrading The Operator-Machine Interface and Annunciation Systems, and the Control Computer Systems at the Pickering GS "A" Nuclear Station

M. T. McPhedran, R. J. Hohendorf, and B. Howard–Computers and Human Factors Engineering Section, Instrumentation and Control Department, Ontario Hydro, 700 University Avenue, Toronto, Ontario M5G 1X6 Canada

Abstract

Unit 1 of Pickering GS "A," Canada's first commercial nuclear power station, entered service in 1971. It features digital computers controlling the nuclear units, the first such commercial application. After approximately 55 reactor years and over 100 computer years of operation, Ontario Hydro is undertaking a major upgrade of the Pickering "A" control computers. The current IBM 1800 computers will be connected to a distributed system of microcomputers which will take over all the major operator-interface and annunciation functions. The upgrade will provide a modern, integrated, operator-machine interface, plus straightforward system expansion and eventual IBM 1800 replacement.

Introduction

The use of computers for plant control was an integral part of the CANDU design from the inception of the Canadian nuclear power program. Control computers have contributed significantly to Ontario Hydro's excellent nuclear plant operation, their performance is regularly among the very best in the world. The first commercial Canadian nuclear unit entered service in 1971 at Ontario Hydro's Pickering GS "A" generating station, a 4 x 540 MW multi-unit CANDU-PHW station. The CANDU-PHW nuclear power system uses horizontal pressure tubes containing the fuel and heavy water coolant. The reactors are fuelled continually at full reactor power.

Pickering "A" features computer control of each nuclear unit, this is done by dedicated minicomputers, which are organized in a dual-redundant configuration. At the Pickering "A" plant computers are used for: reactor and boiler control, overall plant control; fuel handling control; data acquisition and logging; plant monitoring and alarm annunciation. The IBM 1800 minicomputers originally installed for unit control at Pickering "A" are still in use. During 14 plant-years and over 100 CPU years of operation, the IBM 1800 provided excellent performance and very reliable service.

Reasons For The Upgrade

Over the years a significant amount of work was been done to improve the performance and reliability of the control computer systems. However, with time and operating experience, it became clear that certain basic deficiencies existed that could not be corrected in the system as currently constituted. Most of the identified deficiencies were in the computer-associated operator interfaces. Another growing problem was the lack of expansion capacity for all but the most minor new applications. As a result, a detailed joint study was initiated by the Instrumentation and Control Department and Station Operations in 1981. The study, lasting several months, sought to determine the extent and impact of the operator interface deficiencies and to seek the best way to correct them.

Identified Deficiencies and Solutions

The study identified a number of deficiencies and proposed solutions for them.

Alarm Annunciation CRT:

- A single monochrome alarm annunciation CRT is driven by the master computer. The standby computer provides alarm annunciation only via a printer.

Solution: The single monochrome CRT is replaced by two colour CRTs, one driven by the master computer and one by the standby computer.

- Alarms are not categorized by priority or plant systems.

Solution: Alarms are categorized and colour-coded by plant system.

- When the screen is full of alarms, the alarm page is scrolled continuously upwards to add new alarms from the bottom. Under unit upset conditions, the alarms roll up the screen too fast to be read.

Solution: Roll-up is eliminated and the full screen is always readable. Instead, when the screen is full, new message wrap-around from the top of the screen, overwriting the oldest alarms. A degree of alarm grouping is also done to reduce the number of alarms output to the annunciation CRT, especially during upsets.

- A repetitive alarm will fill the screen with "alarm" and "return-to-normal" messages for the same point.

Solution: A single alarm point occupies only one line on the annunciation CRT, even when cycling frequently.

- The output of messages to the CRT and printer is tied together. A message to be output to both devices cannot be displayed until preceding messages are printed, delaying output to the CRT significantly, particularly during unit upsets.

Solution: Output of annunciation messages to the printer and CRT is decoupled.

Printer

- All alarms are printed as they occur. A large volume of paper is produced and must be retained for a minimum period of several months. Later retrieval of specific data is extremely difficult and time consuming.

Solution: Hardcopy is only printed on operator demand. The message generated will be stored on a disc for on-line operator retrieval, and on magnetic tape for long-term retention. Up to nine back pages are available on-line at the operator terminal. The cost reduction in both manpower and material is significant.

- In certain situations, a large number of messages from different categories are mixed together with alarm messages making it difficult to discriminate the alarms, e.g., fuel handling messages on the standby computer.

Solution: Alarms are stored on a disc for off-line historical retrieval grouped by type, i.e., fueling machine, sequence of events, etc.

- The printers are used extensively due to the CRT system limitations, but suffer from legibility problems.

Solution: The printer has been eliminated as a primary source of operator information.

Operator-Computer Interface Panel Deficiencies

- A great deal of information is available to the operator from the computers, but the methods of accessing and presenting information are limited and difficult to use.

Solution: The current operator-computer panel is replaced by a colour operator's terminal. There is ready access to two pages of real-time data updated every 5 seconds. Other previously print-only functions will now be available on the operator terminal, i.e., summaries, historical logs, numeric trend logs, etc.

- Confirmation and checking of operator inputs and requests is awkward. The information is output to the printer located some distance from the operator panel.

Solution: All operator input commands will be via a colour terminal. Confirmation and checking of the operator's requests is provided on the display called up at the operator terminal, as are the operator "prompts."

Expansion Capacity

A major deficiency, identified for some time previous to the study, was the lack of expansion capability in the IBM 1800 computer system. Accordingly, desirable applications could not be implemented in the IBM 1800 computers, and could not be cost justified for a stand-alone system. In any event, stand-alone solutions were considered far from ideal from a human factors standpoint, as the operator information could not be integrated into the existing control computers annunciation system.

Expansion capacity was severely limited or non-existent in a number of areas: (1) no spare analog or digital input capacity; (2) little free core memory space; (3) limited spare processing capacity for certain types of functions due to loading; etc. This meant that there were no practical, effective solutions to the high priority deficiencies identified by the study using the existing computer hardware in its current configuration.

Arising out of the study was a decision to upgrade the control computer systems to correct the identified deficiencies in the operator-computer interface. The major objective of the upgrade was to provide the operator with an effective operator interface based on current human factors engineering knowledge, and to provide expansion capability. Total replacement of the IBM 1800 computer system was ruled out for two reasons: (1) The high reliability of the system (2) The extremely high cost of a total replacement. The main cost components were the extended unit downtime required, the wiring and installation costs for new inputs and outputs, and the associated design costs. The project was given the acronym "PACE".

The Pace Upgrade

The Current Configuration

Each IBM 1800 computer in the existing dual-redundant configuration (fig. 1) is nearly identical, the major functional exceptions are the fuel handling control programs which reside only on the standby computer and are utilized only when this computer is not controlling the unit. The two computers are separately designated the master and standby computers. The master computer is always in control of the unit if it is operational and the control programs are executing correctly. The standby computer takes control of the unit only on failure of the master. The reactor is refueled on-line, under semi-automatic control.

The current operator interface associated with the computer system consists of:

- A single monochrome alpha-numeric alarm annunciation CRT which is driven only by the master computer

- A printer per computer

- A keyboard/printer terminal per computer, based on the IBM Selectric typewriter, for operator control inputs and data log printouts

- An operator interface panel per computer, which is a combination of thumb-wheel switches, push-buttons, and rotary selectors for miscellaneous operator demand functions and a six digit NIXIE tube display

- A CRT on the standby computer used for fuel-handling operations.

The Upgraded System Configuration

The decision was made to upgrade the control computer system by supplementing the existing IBM 1800 computers with a small, powerful, microcomputer-based front-end to off-load all major annunciation and operator-interface functions from the IBM 1800. The basic dual-redundant configuration is retained in the upgraded configuration. Each dual-redundant pair will be made up of a set of multiple computers (fig. 2), called a "channel" for ease of reference, consisting of:

- The current IBM 1800
- A new HUB or Interfacing microcomputer
- A microcomputer, the Annunciation Command Processor (ACP) to process all alarm annunciation messages, drive the operator interface peripherals, and accept all operator inputs.

In addition a single data acquisition (DA) computer is connected to both channels (for new applications).

A communications link is provided between each HUB computer. It replaces the 'data link' between the two IBM 1800 computers, which proved unreliable compared to the rest of the system. It is used to pass key control parameters between the two channels to check that operation of the control programs are synchronized.

Ontario Hydro has undertaken development of a standard microcomputer-based distributed control computer system over the last 4 years which is ongoing. The Pickering "A" computer upgrade is based on a sub-set of this development, and makes use of many of the standard software and hardware modules developed. This distributed system makes use of standard off-the-shelf computer hardware, which is multi-sourced, and uses minimum levels of custom design.

The PACE upgrade to the existing control computers is designed to allow:

- Simple expansion and addition of new applications
- Future upgrades to provide the addition of more sophisticated display features such as graphical trends and barcharts
- Future graceful phased replacement of the functions retained on the present IBM 1800 minicomputers, if necessary due to the deterioration of hardware reliability and/or maintainability.

Other Features of the Pace Design

A number of features incorporated into PACE to assist in system maintenance were selected in consultation with end user maintenance staff, and included:

- Modular components and quick connection cables connected at a single termination panel
- Maintenance mode software to assist in identifying problems and an on-line maintenance display page to identify fault locations
- Permanently installed logic analyzer interface boards on each CPU bus.

While the objective was to minimize custom hardware, some in-house design of hardware was essential. The custom hardware varies in the level of design complexity:

- X.25 communications boards used throughout except for the HUB-IBM 1800 link
- A bootstrap/watchdog timer board
- The HUB-1800 interface, which uses a standard vendor board at the HUB
- The logic analyzer interface

- A termination panel and an audible alarm interface.

Other features of the design were the use of remote system console emulation software to eliminate the need for a terminal for each distributed computer node, and the watchdog/boot board eliminating the need for a bootstrap load device at each node.

The software design makes use of the standard operating system provided by the computer manufacturer and an industry standard high level language, PASCAL, for the applications software.

IBM 1800 Changes

Software: The existing IBM 1800 application programs (such as control programs, etc.) will be retained. Only the outer layer of software will be changed. The programs to be deleted are mostly message formatting routines and drivers for the printers, CRT's and the operator interface panel. The new software, known as "request handling software," must be added to the IBM 1800 to handle communications with the HUB computer and to receive and interpret commands from the operator terminal.

The changes are designed to be transparent to the current software that is retained and any changes to that software are minimized to the greatest possible extent. This is achieved by using the existing software, previously used to service operator demands, as the interface between the new "request handling software" and the applications software.

Hardware: Hardware modifications are minimal and straightforward. The printers, operator interface panels, and the single annunciation CRT are disconnected. Instead, the digital inputs and outputs used to drive these peripheral devices are connected to a custom interface board used for IBM 1800-HUB communications. The board is simple in design and has three main functions: to adjust the HUB-IBM 1800 electrical signal levels; provide optical isolation between the two computers; and provide a means of isolating the HUB from the IBM 1800 for maintenance purposes.

The other change of note to the IBM 1800 hardware was the addition of extra core memory which simplified the software changes. Disturbance of the existing core resident software was minimized and the number of disk-to-core transfers is reduced considerably.

Status of the Project and Future Plans

The current project status is as follows.

- Full system integration testing, of hardware and software, is almost complete. A full channel of hardware has been set up at the station for the testing.
- A fully upgraded standby channel is being installed on Units 1 and 2 at the station. The IBM 1800 master system will be retained in the current configuration until commissioning of the standby channel is successfully completed. It will also serve as a reference during testing.
- A pre-release version of the software will be installed in the Units 1 and 2 standby channels for use by operations prior to full system commissioning.

A major problem in backfitting control computer equipment to an operational nuclear station - the extremely short time-frame for installation and testing during a scheduled outage - is not an issue for Units 1 and 2. Both units are undergoing major overhauls and will not return to service until about mid-to-late 1986. This will be an issue for Units 3 and 4, as installation of the new computer hardware and software is targeted for relatively short (30-40 day) scheduled annual maintenance outages. With the experience gained on Units 1 and 2, no major problems are foreseen.

The scope of the current PACE project was limited by the economic climate and funds available at the time the project was approved. However, the system design configuration allows for future upgrades and renovations in a straightforward, cost effective manner.

Further upgrading of the operator interface will be examined once the PACE project is completed. Potential additions include providing graphical trends and barcharts, process diagrams and process related displays, and annunciation and/or display CRT's located at major process control panels e.g., reactor, boiler, etc. The addition of new applications, such as generator temperature monitoring, will also be reviewed.

A step has already been taken in the direction of adding new applications. The data acquisition (DA) computer allowed the annunciation for two major new station systems to be integrated into the overall PACE computer annunciation system in a fairly simple manner. One of the systems, the emergency coolant injection (ECI) system, is safety related, and would otherwise have been implemented as a stand-alone annunciation system, which was undesirable.

While the scope of the PACE project itself is limited in its present form it provides the vehicle for future expansion at the station. Of greater significance, it provides the basis for a straightforward, staged replacement of the remaining IBM 1800 applications, with greatly reduced costs, schedules and disruption of unit operations. Non-control applications would migrate first to the DA computer and control programs would then be removed one at a time, likely to separate dual-redundant distributed nodes.

There are three Hydro nuclear stations using obsolete computer hardware. All are candidates for eventual replacement of their control computer systems. The PACE project will provide valuable experience in this exercise and a potential computer system to form the core of the replacement. Our aim is to provide standardized systems across our plant population in the future to ease the problems of replacing existing systems and having to maintain many diverse systems.

The scheduled in-service date for the first unit, Unit 1, is December 1, 1985.

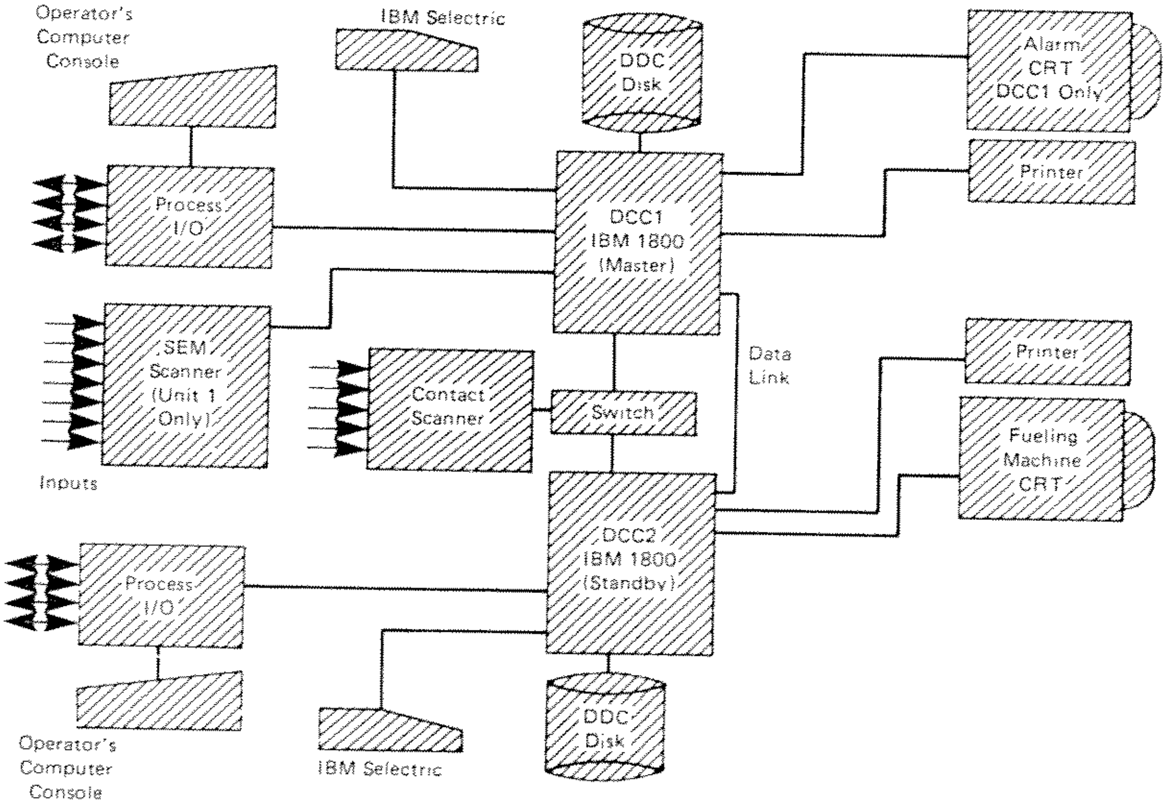

Figure 1. Pickering GS A Control Computer Configuration.

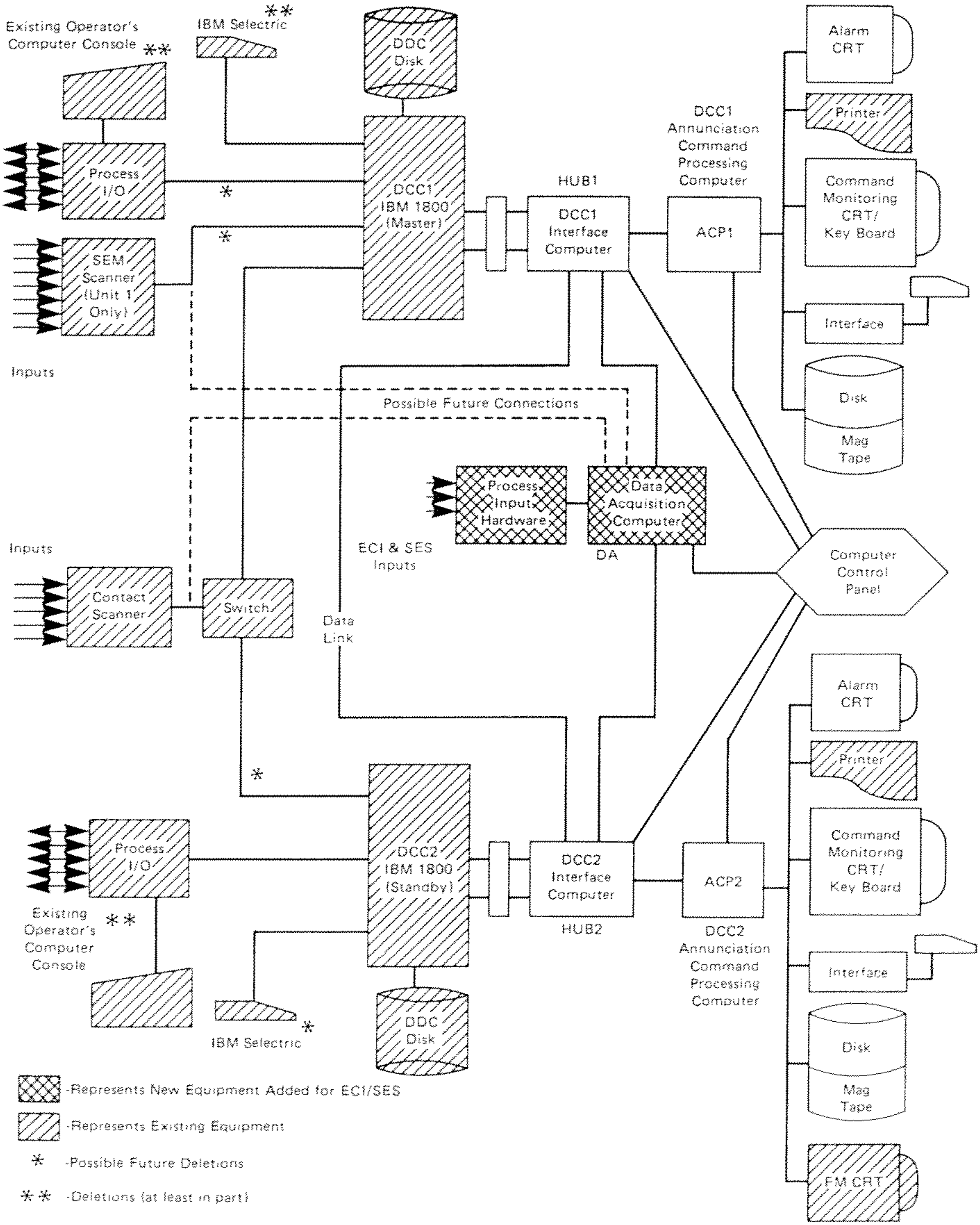
Existing Operator's Computer Console **
IBM Selectric **
DDC Disk
Process I/O
*
*
DCC1 IBM 1800 (Master)
SEM Scanner (Unit 1 Only)
Inputs
HUB1
DCC1 Interface Computer
DCC1 Annunciation Command Processing Computer
ACP1
Alarm CRT
Printer
Command Monitoring CRT/ Key Board
Interface
Disk
Mag Tape
Possible Future Connections
Process Input Hardware
Data Acquisition Computer
DA
ECI & SES Inputs
Computer Control Panel
Inputs
Contact Scanner
Switch
Data Link
*
Alarm CRT
Printer
Command Monitoring CRT/ Key Board
Process I/O
DCC2 IBM 1800 (Standby)
DCC2 Interface Computer
HUB2
ACP2
DCC2 Annunciation Command Processing Computer
Existing Operator's Computer Console **
Interface
IBM Selectric *
DDC Disk
Disk
Mag Tape
FM CRT
▩ -Represents New Equipment Added for ECI/SES
▨ -Represents Existing Equipment
* -Possible Future Deletions
** -Deletions (at least in part)

Figure 2. Upgraded Computer Configuration.