THAI - CANADIAN
NUCLEAR HUMAN RESOURCES DEVELOPMENT
TRAINING PROGRAM

EFFECTIVE TECHNIQUES
IN
CONFIGURATION MANAGEMENT
OF
NUCLEAR POWER PLANTS

LECTURE NOTES FOR THE COURSE ON

PEER EVALUATION TECHNIQUES

BY: R.B.TAYLOR

November 1997

CONFIGURATION MANAGEMENT

1.0 OBJECTIVE OF PRESENTATION

Methods used to ensure plant configuration management, including the use of administrative controls, thorough review of temporary and permanent changes to the plant, and comprehensive routine testing are discussed. This discussion includes methods used to control computer changes.

Ways in which plant and equipment can be taken out of service and returned to service in a controlled manner are identified and the importance of post maintenance testing is emphasized.

This lecture concentrates on the aspects of configuration management that are most relevant to plant operation. Design aspects are not discussed in detail.

2.0 GENERAL

Plant configuration management is an integrated process that (a) identifies existing approved plant specific design requirements and (b) controls change to ensure that selected plant structures, systems, components, and control computer software conform to the approved design requirements. These design requirements are the current functional and operational requirements for the plant, as determined by the design authority, and approved by the regulatory authority.

Additionally, the plant's physical and functional characteristics must be accurately reflected in selected plant documents such as design, procurement, operating, testing, maintenance, and training documents.

In summary, it provides the information base to enable the plant to be in an analyzed safe state at all times

A configuration management control program includes an evaluation process which identifies, examines and selects plant hardware, computer software, and documents that will be part of the management program. The evaluation process also provides for periodic assessment of the program elements throughout the lifetime of the program.

Typical examples of documents included in a configuration management program would be as follows:

- system descriptions;
- drawings;
- fundamental design criteria;
- special studies and reports;
- procedures, guidelines, and acceptance criteria;
- quality assurance and quality control documents;
- codes and standards;
- vendor manuals;
- licensing commitments;

- safety report;
- modification packages;
- instrument and control set points;
- component lists;
- purchase orders;
- regulatory guides;
- equipment performance and maintenance records;
- welding qualification records;
- design requirements. They should be continuously updated to include all approved changes and should be accurately reflected in output documents such as drawings, system descriptions, specifications and procedures as determined by the utility.
- modification, or change control ensures that changes to the facility are correctly identified, screened, designed, evaluated, implemented, and recorded. this includes both permanent and temporary changes. it must also ensure adequate documentation and control of the situation, where the design has been changed, but the change has not yet been installed at the plant;
- documentation control identifies, stores, updates and retrieves important plant documents throughout the lifetime of the plant;

A well defined and managed configuration control process is required for the following reasons:

- to ensure that all relevant station documents are consistent with the plant specific design requirements;
- to ensure that the many changes which take place to the design during the life cycle of the plant are based on current, plant specific knowledge of the configuration of plant hardware, software and design documents;
- to ensure that the procurement of materials and spare parts is consistent with the current design configuration;
- to ensure that the operating license is based on the current design configuration;
- to ensure that the plant documentation accurately reflects the plant configuration.

3.0 PLANT INVOLVEMENT IN THE CONFIGURATION MANAGEMENT PROCESS

The aspects of configuration management that the plant is most involved in are as follows:

- reviewing proposed design changes;
- controlling the installation of permanent and temporary changes;
- commissioning and testing the changes to ensure that they meet the design intent;
- ensuring that the plant is operated and maintained in the appropriate configuration;
- maintenance of documents and records.

Each of these aspects is now considered in more detail.

3.1 Reviewing proposed design changes

Plant modifications can be initiated by operating or design organizations. Although modifications should be minimized, they are frequently necessary to:

- take full advantage of operating experience;
- satisfy new regulatory requirements;
- benefit from technological advances either with respect to equipment, or with respect to performance analysis;
- replace obsolete equipment for which spares are no longer available;
- improve operability or maintainability;
- improve safety and / or economics.

It is important that the station personnel are involved in evaluation of proposed changes from the concept stage, to ensure that the final design will appropriately consider operating aspects. For example:

- what are the operating difficulties caused by the change? A change which turned reactor trim rods into shutdown rods made subsequent spatial power control more difficult.
- does the station have the skills necessary to maintain the new equipment? Will additional staff be required? A change which brought in very sophisticated new electronic equipment could not be maintained by the station staff. Outages were caused by breakdown of the equipment.
- will long outages be required to install the equipment?
- where will the modification be located? What is the impact on access to other equipment/ systems?
- what will be the impact on operation of other equipment or systems? For example changing the capacity of heat exchangers on one system will impact on the operation of the system providing cooling water to those heat exchangers;
- has adequate access been provided to operate the equipment?
- are the controls located appropriately in the control room?

Appropriate consideration of operating aspects at the design stage may make subsequent configuration control at the plant much easier.

3.2 CONTROLLING THE INSTALLATION OF PERMANENT AND TEMPORARY CHANGES

The following sequence of activities is important when carrying out either temporary or permanent changes:

- the change must be properly reviewed, approved and documented. The appropriate documentation includes design information, installation information, equipment lists, revised operating instruction, revised training material and testing / commissioning requirements. It is important that the status of other design changes is also reviewed, because one change may assume that an earlier proposed change has already been installed. This may not be the case due to the long time between planned outages and the changes in plant priorities. This becomes more complex on multi-unit

stations, where each unit will be in a unique status with respect to previous design changes;

- the reactor is placed in a safe operating state for the change being installed. For example changes to the regulating system may require the reactor to be in a guaranteed shutdown state;
- the system is placed in an appropriate state. The complete system may need to be shut down or perhaps only a part of it, depending on the complexity of the change;
- equipment is correctly isolated;
- change is installed;
- quality assurance checks are completed;
- testing and commissioning are completed and the results reviewed to ensure that the design intent of the change has been fulfilled;
- system is returned to service.

3.2.1. Changes to computer programs

Changes to computer programs follow the same general sequence of events as shown above, but they present unique challenges and are therefore dealt with in more detail.

In the Canadian environment, computers are used for the following functions in the control of nuclear power plants:

- reactor power regulation;
- boiler pressure control;
- reactor power stepback;
- moderator temperature control;
- thermal power calculation;
- turbine automatic run-up;
- on power fueling;
- alarm processing;
- channel temperature monitoring;
- operator interface.

On the most recently commissioned plant, they are also used for reactor protective system (scram) control and testing.

Each plant has two main control computers which duplicate key control functions such as reactor power regulation and boiler pressure control. Automatic control transfer occurs between the master computer and the back up computer, if the master is not functioning correctly.

In addition to the two control computers there is a third computer which is off line and is used for off line testing.

It can therefore be seen that these computers perform many important functions in the plant. They are also subjected to frequent changes, since they interface with many plant systems.

The computer change process is as follows:

need for change is identified
↓
change package produced
↓
conceptual change approved
↓
software coded
↓
test plan produced
↓
coding independently verified
↓
test plan independently verified
↓
off line testing complete
↓
installation plan produced
↓
installation plan verified and approved
↓
confirm unit suitable for installation
↓
install in first computer
↓
independently verify first computer
↓
test first computer
↓
wait to evaluate impact
↓
install in second computer
↓
independently verify second computer
↓
test second computer
↓
review change effectiveness
↓
update software library

It has been found that identification of the exact nature of the proposed change is important. For example, one requested change asked for a program to recognize a reactor trip if two of three reactor trip signals were received. It did just that, and did not recognize three of three reactor trip signals as a reactor trip.

3.2.2 Control of temporary changes

A temporary change is any short term alteration made to the plant systems, structures, or equipment that does not conform with approved drawings or other design documents.

The following are examples of temporary changes:

- lifted wires;
- electrical temporary changes;
- disabled annunciators;
- modified pipework;
- temporary set point changes;
- installed or removed blank flanges. i.e. not according to drawing;
- installed or removed filters or strainers;
- plugged floor drains;
- temporary pipe supports.

A station program to control temporary changes should include the following elements:

- the number of temporary changes must be kept to a minimum;
- changes must be approved by an individual who is knowledgeable of the impact of the temporary change on configuration of the plant;
- changes must be properly identified in the field and in plant documentation such as flowsheets, operating manuals, and maintenance manuals;
- appropriate training on the existence of the temporary change and it's consequences must be given;
- temporary changes must have a limited lifetime, and must be routinely evaluated by senior plant personnel;
- installation of temporary changes should be independently verified to ensure that they are correctly installed, where appropriate;
- the plant should be routinely checked to ensure that unapproved temporary changes are not installed in plant systems.

3.2.3 The commissioning and testing of changes

It is important that the commissioning and testing requirements check that the design change has achieved its intent and that they also determine that there are no unpredicted consequences. This is particularly important when the change impacts on systems that were not changed, but are nevertheless affected by the change. This is often an issue with common service systems such as electrical, instrument air, or service water. For example, a change to a heat exchanger capacity may result in the need to run an additional service water pump. This may cause all of the running pumps to run at higher vibration levels, because they are at a less desirable point on their performance curves.

3.2.4 Maintaining configuration control during operation and maintenance

In order to ensure that the plant remains in the appropriate configuration during its operating life cycle, it is necessary that operating and maintenance practices conform to the design intent. This is achieved in Canada by doing all operating and maintenance work according to a procedure. These procedures are normally the operating and maintenance

manuals, but they can be modified by approval of supervisors. The supervisors must have the appropriate training to enable them to determine that the proposed temporary procedure is consistent with the design intent.

Another important aspect of maintaining configuration control is by ensuring that routine testing is rigorously carried out according to a procedure. This gives assurance that critical parameters are in the state predicted by the design analysis, and their state has not been changed in error or due to equipment breakdown.

Post maintenance testing must be carried out to ensure that maintenance has not caused the plant to deviate from the design intent.

This subject of maintaining configuration control in operation and maintenance is discussed further in the lecture on operations.

The defense in depth philosophy requires that more critical procedures must have multiple reviews, to limit the possibility of human error.

4.0 OSART EXPERIENCE

Maintaining a completely effective configuration control programme is difficult and demands significant attention to detail. OSART findings are frequent in the area of documentation management, plant labelling, procedural compliance, control of temporary changes and rigorous testing processes. In some cases the findings indicate minor weaknesses in the system and in others the problems are more widespread.