OCCURRENCES IN CONTROL ROOM EQUIPMENT, PROCEDURES AND PERSONNEL PERFORMANCES: IRS CONTROL ROOM EVENTS

V. Tolstykh
International Atomic Energy Agency (IAEA)
Vienna, Austria

ABSTRACT

The IAEA/NEA Incident Reporting system (IRS) was established in the early 1980s, its objective being to gain from operating experience achieved in countries with nuclear power programmes by means of exchanging information on events relevant to safety.

Among the 2171 events in the database, 175 events (i.e. 8%) were identified as "control room events". It was decided to group these into three sets for further study: 65 events with common mode/cause failures (CCFs), 22 events with cognitive errors and 39 events with unforeseen interaction between NPP systems.

It is expected that the pitfalls experienced in the IRS and the questions derived from this study will help to gain a better understanding of the needs and interests of specialists in advanced information methods and artificial intelligence in NPP control rooms.

1. INTRODUCTION

The IAEA/NEA Incident Reporting System (IRS) was established in the early eighties, its objective being to gain from the operating experience achieved in countries with nuclear power programmes by means of exchanging information on events relevant to safety. The IRS is based on the principle that each participant country promptly provides detailed information on the experience it has gained from unusual events occurring in its nuclear power plants, and makes this data available to all other IRS participants. The selection of events to be reported corresponds to internationally agreed categories covering main issues. To facilitate the storage and retrieval of reports transmitted to the IRS, which now exceed 2000, a database is maintained to enable searches from a range of set IRS queries. Currently, IRS information (i.e. original reports, technical reviews and studies) is being circulated to 28 countries.

NPP events and relevant lessons reported to the IRS could provide valuable information to specialists in advanced information methods and artificial intelligence in NPP control rooms. All findings from IRS data should be used bearing in mind that (a) the IRS collection of events is incomplete, and (b) there are some limitations in the IRS classification scheme and search capabilities.

Common cause failures, cognitive errors and unforeseen interaction between NPP systems in occurrences in control room events were chosen in the first line to meet the needs and interests in the area of NPP computerized process control.

2. RESULTS OF SEARCHES FOR CONTROL ROOM EVENTS REPORTED TO THE IRS

Of the 2171 events in the database, 175 events were identified as control room events (i.e. 8%).

The IRS classification scheme (Appendix 1) and engineering judgement were used to select:

- 28 events in which main control room equipment was affected;
- 63 events involving procedural deficiencies; and
- 69 events involving NPP operator errors.

This set of IRS events was studied to make general observations and findings. Subsequently, control room events were regrouped with the following results:

- 65 events with common mode/cause failures (CCFs);
- 22 events with cognitive errors;
- 39 events with unforeseen interaction between NPP systems.

3. IRS PITFALLS AND QUESTIONS

IRS facts and lessons were treated accordingly to support and encourage a questioning attitude in specialists in advanced process control in NPPs.

Experience in operating plants has shown that plant computers need to be replaced every 10-15 years, meaning that the plant will run with at least three different generations of computers. For example, in Canada second generation control rooms were installed in CANDU plants designed in the mid-seventies and early eighties. Third generation features will be incorporated in the CANDU 3 station design and future CANDU stations.

Since IRS data cover a period of approximately 15 years, they should be attributed mainly to the first and second generation control room. This is a weak point in the IRS data for the present study.

3.1 Common cause failures in control room events reported to the IRS

Failure of a number of devices and components to perform their functions may occur as a result of a single specific event or cause.

CCFs are now a burning issue in nuclear safety. Applications of advanced information methods and artificial intelligence in NPP control rooms could increase the potential for common cause failures and could introduce new features of CCF.

As a starting point, a brief excerpt from an IRS report on loss of offsite power caused by problems in fibre optic systems is provided as follows:

While in hot shutdown, the unit experienced a trip of two preferred station transformers; about one hour later, the other two preferred transformers tripped. The emergency diesel generators started as designed and the emergency safety features system actuated. Within two hours, normal power was restored. Investigations showed that this event involving loss of offsite power was not caused by a valid signal. Testing showed that hand held radios could have caused the event when keyed near the transmitters and receivers for the fibre optics system. The corrective measures taken included: shielding of the fibre optics system; posting signs to prohibit the use of radios near the fibre optics equipment; rewiring the equipment so that two channels are required for tripping; and providing control room annunciation of the system's status.

The following examples, in condensed form, are provided to illustrate common cause failures in control room events:

- The unit was operating at 100% power when a loud noise was heard in the main steam check valve vault. The control room indications were normal, however.

- Inadvertent drainage of spent fuel pools was caused by a valve left open two days previously after other activities had been carried out. No alarms were activated in the control room as the level indicator in the spent fuel pool was inoperable.

- There was a lack in the indication that and when the required safety equipment became inoperable. Very often safety equipment is "awaiting" equipment; safety systems may remain inoperable for a long period until their conditions are discovered through testing or initiation of an actuation signal.

Conclusion: The indication system in NPP control rooms is incomplete.

- A voltage drop occurred followed by the loss of train of a 48 volt bus leading to loss of both off-site power and and the train of a diesel generator. A low voltage alarm went off in the control room but was not noticed as it was grouped with five other less important alarms related to faulty insulation defects, and these had been flashing frequently.

- There was a complete loss of the remote cabinets containing multiple circuit cards for the control of visual and audible annunciator functions in the main control room because of fire. There was also a lack of specific emergency operating procedures.

- Deficiencies were discovered in design, operation and maintenance of the control room boundary and the emergency ventilation system provided to maintain control room habitability during a design basis accident or toxic gas release. There were occurrences with total loss of main control room cooling.

- Cases had occurred indicating difficulties to control, either automatically or manually, the safety-related breakers with automatic logic from the control room; difficulties arising from poor co-ordination between control room personnel and other personnel, e.g. incorrect signals, wrong connections of computer cables; difficulties due to total or partial loss of control room instrumentation because of loss of power supply.

3.2 Cognitive aspects of control room events reported to the IRS

The fundamental unfeasibility of describing all possible situations in NPPs could lead to an incorrect identification of a situation and, as a consequence, an incorrect selection of control instructions and decisions. Examples of the most frequent cases with cognitive errors reported to the IRS are:

- Intentional bypassing of the automatic actuation of plant protective features because the operators were misled by an inaccurate diagnosis of plant conditions (e.g. by an erroneous indication that the spray valve is in a closed position).

- The auxiliary operator performed some maintenance work without informing the control room. Since the reactor operator in the control room was unaware of the status of the NPP systems, he took the wrong actions which in turn led to serious consequences.

- The normal control room indicator for feedwater pump suction pressure had failed and was tagged for maintenance. An operator who had been sent to check the local suction pressure indicator did not communicate the actual pressure to the control room. As a result, a faulty indication was used by the operating crew in their actions (finally causing a reactor trip).

Conclusion: In many cases, cognitive errors were caused by wrong actions being taken by other persons, by wrong logic and malfunction of the NPP systems.

- The control rod was improperly manipulated. Various unauthorized methods (i.e. the use of the emergency rod in the position switch; the use of individual scram switches) were applied to speed up rod insertion and rods were consequently inserted in the wrong sequence. The cause was poor operator judgement and insufficient guidance.

Problem: There are more possibilities of, excuses and justification for poor operator judgement and insufficient guidance in the case of the advanced control room.

- Some events reported illustrate discrepancies in the knowledge of the control room operator and that of the field operator (this possibly being a source of wrong actions). There is a tendency towards placing more emphasis on knowledge-based work than on working according to the rules and tradition. Therefore, the control room operator will become more and more intellectual.

- A partial loss of control room lighting (and a loss of non-safety related parameter indications) caused the control room operator to believe that a reactor trip was occurring and that the plant had lost a good part of its power supply. For these reasons, the operator manually tripped the reactor and turbine. Simple reasons for cognitive errors should not be overlooked.

3.3 Unforeseen interactions in control room events reported to the IRS

There is a category in the IRS classification scheme titled: "Unforeseen or significant interaction between systems". As a rule, IRS reports assigned to this category are sources of information on hidden failure paths. Thirty-nine

events were identified and examined under this category, most of which provide information on unforeseen interaction between the NPP systems whereby the control room did not play a leading role. IRS findings in this area include the following:

- If a fire should occur in the control room (or in the cable spreading room) power would have to be removed from the valve motor operators in the residual heat removal (RHR). If the damage occurred prior to removing power, the valves would suddenly open and cause over-pressurization of the RHR piping leading to a LOCA that could not be isolated.

- Cases have been reported in which there was no indication in the control to suggest malfunction of the NPP system (e.g., the auxiliary feedwater pump cavitation); there were unexpected effects of interconnecting of ventilation flows regarding control rooms; there was spurious indication of "loss of rector coolant flow"; wiring errors.

4. CONCLUSION

The IRS framework can undoubtedly provide useful information to specialists in advanced information methods and artificial intelligence in NPP control rooms. A special IRS topical study should be organized jointly by IRS experts and said specialists.