Investigation of Accelerator Incidents – Regulatory Perspective

Abdul Alwani
Senior Project Officer
Processing and Research Facilities Division
Canadian Nuclear Safety Commission
Ottawa, Ontario, Canada
abdul.alwani@cnsc-ccsn.gc.ca

Abstract
The probability of incidents and accidents exists during the operation of particle accelerator facilities. Particle accelerators are a type of nuclear facility that is regulated by the Canadian Nuclear Safety Commission, the federal regulatory agency of nuclear materials and facilities in Canada. Safe operation of an accelerator involves not only avoiding incidents but learning from them to avoid future recurrences.
This paper describes the regulatory expectations in Canada with regard to responding to incidents and near misses. This includes putting in place incident handling and investigation systems and procedures. Also, reporting requirements on events and corrective actions are mentioned. An example of an event that occurred at a Canadian accelerator facility is provided in the paper.

Keywords
Regulatory oversight, incident investigation, accelerator safety

INTRODUCTION

The Canadian Nuclear Safety Commission (CNSC) is an independent federal government agency that regulates the use of nuclear energy and material to protect health, safety, security and the environment and ensures that Canada's international commitments on the peaceful use of nuclear energy are respected. Particle accelerator facilities in Canada are considered nuclear facilities as per the *Nuclear Safety and Control Act*. The Act requires the issuance of a licence for preparing a site, constructing, operating, modifying, decommissioning or abandoning a nuclear facility. Also, it requires licences for possessing, transferring, or using a nuclear substance. A facility licence normally covers one or several accelerators on one site and nuclear substances and devices associated with the accelerators.

In addition to issuing licences based on careful review and assessment of the safety aspects of the design and operation of the facilities, the CNSC conducts regulatory compliance activities aiming at promoting compliance with the regulations and enhancing good safety practices, verifying compliance with the safety and regulatory requirements and enforcing compliance if required.

Under this regulatory regime, the licensee is fully responsible for the safety of its facility. This is reflected in the verification and enforcement aspects of the regulatory compliance oversight. The promotion aspect however, plays an important role in the compliance program. The CNSC views the safety culture at the licensed facilities, whether among the operating organization staff or management, a major factor in moving the safety forward and continuously upgrading the safety standards to ensure safe operation.

OPERATING EXPERIENCE

At the licensing stage of a nuclear facility, the CNSC reviews the design, the safety features and the proposed operating limits and conditions of the proposed facility. In addition, the CNSC looks at the operational aspects including training, operational procedures, and emergency response protocols. The management oversight and structure are also assessed to confirm that the licensee is qualified to conduct the proposed nuclear activities.

At the licensing stage, for initial operation or modification the CNSC requires a safety analysis identifying the credible accident scenarios expected in the lifetime of the facility and assessing their possible consequences. The purpose of this requirement is to come up with a conclusion regarding the overall risk imposed by the facility operation to the public, workers and the environment.

As part of the CNSC's expectations the licensee is required to establish an operating experience (OPEX) program. The main objective of the OPEX program is to ensure that the licensee draw lessons from its operation to improve safety and prevent recurrence of hazardous situations. Lessons are drawn from accidents, incidents, and unusual occurrences including unplanned events that did not result in injury, illness, or damage - but had the potential to do so.

A licensee may have elements of an OPEX program embedded in other programs such as quality management systems and non-conformance procedures. Due to the CNSC's regulatory mandate, the CNSC distinguishes between safety consequences and operational consequences; although the licensee may devise the same system or program to deal with both types of undesired consequences.

INCIDENT INVESTIGATION SYSTEM

Both the quality of the investigations and the mechanism to learn from the investigations and provide inputs to the OPEX program are essential for effective

learning and successful prevention of repeat of incidents. The CNSC accelerator licensees are expected to have in place a formal, systematic, comprehensive, and objective process for the investigation of significant events. In order to prevent recurrence of events it is necessary to analyze events for the purpose of identifying the root cause(s). Once these root causes have been rectified, the probability of the event being repeated is low.

A structured approach to event analysis is a must. The licensees are dissuaded from investigations on an intuitive basis. This is to avoid event investigation results wherein it is much more difficult to get a clear picture of what happened, how it happened, and why it happened. In addition, the corrective actions in such an approach are usually insufficient or inappropriate to prevent recurrence. The CNSC requests that licensees put in place a comprehensive, systematic approach to event analysis.

ROOT CAUSE ANALYSIS

The greatest threat to a nuclear facility comprised of people, hardware and organizational structures, is from the accumulation of delayed-action hidden failures or "latent" failures in the system, most of which originate from the organizational and managerial sectors. A latent failure is either a decision or action with damaging consequences which may lie dormant within the system for a long time. These weaknesses only become evident when they combine with a local triggering factor such as active failure, technical fault, or atypical system conditions. In many cases they originate from people whose activities are removed from the human-machine interface such as designers or managers. The more complex, interactive and opaque the system, the greater will be the number of latent failures. In addition, if we move higher in the organization, the greater the opportunity exists for generating latent failures and the broader the reach of these failures. In a highly protected system, the probability of an isolated action leading to an accident is very small. But, several causal factors can create a "trajectory of opportunity" through the multiple defences. In summary, latent failures may lie dormant in the system until a trigger initiates an accident sequence. Thus, the main thrust of accident prevention programs should be aimed at eliminating these failures.

There are various methods used by the CNSC licensees to conduct root cause analysis. Two examples are: a) Institute of Nuclear Power Operations' (INPO) Human Performance Enhancement System (HPES), and b) System Improvements' TapRooT$^{@}$. Both are means by which the fundamental causes of failure may be determined. Such analysis involves the examination of an event from the perspective of human behaviour, and makes use not only of documentation but also of behaviourally oriented investigative techniques. This type of approach allows the analyst to determine both the HOWs and the WHYs in any event situation.

It is not sufficient for a team of managers, supervisors or operations personnel to form a working group to discuss what they think happened during the event, and then make recommendations on the basis of that discussion. Rather, the use of a formal method for event analysis is necessary. The use of an objective, structured and systematic approach ensures that investigators will proceed through data gathering, analysis, evaluation, recommendation and follow-up phases using appropriate techniques and mechanisms. While only those elements which are relevant to the incident should be included in an investigation, this is not to say that it should be narrowly focused. An investigation should be comprehensive in order to consider the "bigger picture".

In addition, the relationships between the various elements must be considered in a human performance related analysis. No one element stands alone. Events are seldom as simple as they may seem at first glance, and what may appear to be a simple operator error may stem from difficulties relating to supervision, management or work practice. The application of a structured, systematic and comprehensive approach allows investigators to isolate those elements which pertain to the situation at hand, and to examine the interconnections between them. In addition, it should be noted that the causes of major events are often the same causes for minor events, and that an inappropriate behaviour at the management level can have much broader-reaching effects than an inappropriate behaviour at the operator level.

A root cause is a fundamental cause which, if corrected, will prevent recurrence of an event or condition. Usually human performance events do not result from just one root cause. Often a significant event results from the combination of two or more causal factors which combine synergistically to produce the undesirable results. The accurate identification of root causes is of prime importance if one is to reduce human error and prevent event recurrence in nuclear facilities. Management can play a key role in the identification and correction of event causes through the application of non-punitive systems such as HPES or TapRooT$^{@}$. Clearly, the objective of such methods is to identify pre-disposing error conditions and eliminate them. This in turn leads to reduction in downtime and long-term economic benefits.

The HPES/TapRooT$^{@}$ investigations involve examining conditions prior to, during, and after the event, the human behavioural factors (the human-specific symptoms of the problem), and the work environment.

When a licensee report, for instance, mentions that "…This incident seems to have been caused by an unfortunate combination of events that have not occurred before...". The CNSC typically responds by pointing out that this is the usual mechanism for failure. Each of the contributors to the significant event is known as a "latent failure" because it exists in the system for some time before the genesis of a significant event. Once several of these latent failures line up in a

particular configuration, a significant event occurs. Significant events usually result from a combination of root causes "latent failures". The identification of these latent failures through root cause analysis enables one to correct these failures and thereby avoid significant events.

CONSIDERATIONS FOR EFFECTIVE INCIDENT INVESTIGATION

From the regulatory perspective and experience the following considerations are frequently raised and recommended or required from the accelerator licensees:

Independency

There are pluses and minuses for involving persons from outside the operation and management circle in any investigation. The CNSC views the advantages far outweigh the disadvantages of this approach. First, there is a need for looking "outside the box" or having the wide perspective when looking at a particular event subject to an investigation. The individuals directly involved tend to be focusing on particular areas and details without stepping back and raising questions about the adequacy or inadequacy of procedures, work arrangements, or training for instance.

Also, the group involved may be perceived as in a conflict of interest situation and despite their usual sincerity in the process, having an independent investigation normally eliminates any suspicion of conflict of interest.

This may or may not be practical or possible depending on the situation. In such cases a team combined of a mixture of people from within the involved group/management and from outside would be recommended.

Promptness

People tend to forget what happened the further they are away from the event. Also, the data may not be fully preserved with the passage of time. In addition, when workers talk the incident over they may unintentionally influence each other's recollection of the event. It is highly recommended to launch the investigation quickly after the incident. As a minimum, whatever data and information may be helpful to the investigation should be preserved as much as possible.

Expertise

The CNSC licensees are encouraged to have trained staff on one or more methodologies of incident investigation. In addition, it is recommended to have a "committee" ready to be called upon to investigate significant incidents. Depending on the size of the operating organization, a dedicated staff member or group may not be possible and having a "part-time" investigation team has shown to be very effective at times.

Corrective Actions

Following identifying the apparent causes and root causes the investigation should conclude with recommendations for corrective actions. Normally, urgent corrective actions are completed quickly and possibly as part of the emergency response to the incident. The report of the investigation in this case merely summarizes those immediate corrective actions. In addition, the investigation should provide, from the investigators' perspective, a recommended set of changes and/or actions to improve safety and prevent recurrence.

The scope of the corrective action should be appropriate to the root cause. If the root cause is generic and extends beyond the affected part of the facility or operation in question, the corrective action should extend as well. For instance, if the root cause is a lack of effective management oversight in the facility, the corrective action should be handling the overall oversight.

The corrective actions should be tied to a time frame based on feasibility and most importantly based on risk. Although it is not an exact science, the safety assessment should look into what priorities should be given to various corrective actions and the action plan should justify the schedule based on bringing the risk to an acceptable level.

Management Responsibilities

The facility management has important responsibilities with regard to incident investigations and follow-ups.

- First, the management should ensure that the investigation process has been followed and the results are sound.
- Second, the management should make a decision with regards to the recommended corrective actions. The investigators may provide a wish list of improvements which the management may not be able to implement due to budgetary or other constraints. Therefore, the management should ensure that, at the minimum, sufficient and necessary actions will be implemented to correct the deficiencies.
- Third, the management should monitor the implementation and follow-up on completing the actions.
- And finally, due to the position of the management in the organization they may be in a better position to ask the questions about potentially similar deficiencies in other parts of the organization and see the generic aspect of the deficiencies.

Graded Approach

Root cause analyses and full investigations can be expensive and draw a lot of resources. Not all incidents or events need to be investigated or fully investigated. The consequences of an unusual event in a nuclear facility can be significant, potentially significant or not significant. The CNSC recommends that the licensees devise their own classifications of the events for the

purpose of the extent of the investigation and follow-up required.

No classification of events is perfect and there is usually a grey area where the CNSC requires the licensees to err on the side of caution and, when in doubt, consult with the regulator and elevate the requirement. It is also possible that an incident may not have any potential negative consequences by itself but needs particular attention because it might reveal weaknesses in other areas of safety significance. For instance, a programming error in a non safety related system may raise concerns of possible errors in other systems with safety importance programmed by the same person or group.

REGULATORY FOLLOW-UP PRACTICE

The CNSC requires that the accelerator licensees report certain events and occurrences of safety or compliance significance. Reporting requirements for a specific facility are defined in its operating licence. Below is an excerpt from a typical licence regarding reporting requirements:

The licensee shall make reports to the Commission…. of any:

(a) failure of equipment or procedures which led to or which, in the absence of safety systems provided, could have led to any release of radioactive material from the facility;

(b) failure of a safety or safety-related system which did prevent or could have prevented the system from performing its intended safety function as described in the [licensing] documents… or meeting the conditions for safe operation defined in the [licensing] documents…;

(c) inaccuracy or incompleteness in the [licensing] documents …that could affect the results of the safety assessment in these documents;

(d) hazard different in nature or greater in probability or magnitude than that described in the [licensing] documents …; and

(e) event that constitutes or reveals a violation of any conditions of this licence, the Nuclear Safety and Control Act or its Regulations.

Usually a verbal report is required within 24 hours and a preliminary written report is required within ten business days. There is no pre-imposed deadline on final reports. This was made specifically to ensure that the priority is given to conduct a thorough investigation rather than filing by a deadline.

The licensee reporting an incident will launch a CNSC follow-up. Below are some highlights of the main issues of concern to the CNSC.

Emergency Response

The CNSC follow-up to a reported event consists of answering a number of questions such as: Is the emergency situation over or is it continuing? Has the licensee responded adequately to the emergency? What assurance is there that the emergency situation has terminated? In accelerator facilities there are very few scenarios in which an emergency may last for an extended period of time and usually the incident follow-up will occur after the emergency situation ended.

Consequences

What are the consequences of the incident in terms of injuries, radiation doses, contamination to persons, or to the environment? In many cases, the data needed to quantify the impact or reconstruct the facts are perishable, including the recollection of the people involved of the incident details and the length of time they have been exposed to high fields of radiation for instance. Of course, personnel dosimetry data will be the first and most reliable source of information to arrive at the estimates.

Assessing the consequences is important in many respects. It allows one to see whether remedial actions are needed. In addition, it helps grading the severity of the event which will be a factor in assessing the long-term response and corrective actions.

Incident vs. Safety Case

The basis for licensing an accelerator facility is normally documented in one or several safety analysis reports which document the facility's safety case. The safety analysis section of a safety report should include several operational and unusual scenarios with various degrees of probability. Certain scenarios of incidents are assumed the bounding scenarios since they suggest the most critical and severe consequences. These incidents and accidents are analysed in the safety report with certain conclusions that the risks from each bounding event is acceptable.

During the writing of the safety analysis report, the analysis assumptions are not fully validated or, sometimes, there is limited knowledge of the system behaviour in the situations. The licensee is requested to review the actual incident scenario and compare it with the safety case. Then, the licensee should adjust the case and its assumptions if required. This is to reconfirm that with the new knowledge gained by the incident, the revised safety case is acceptable. If it is not, the facility is no longer justified to operate from the safety view point.

Corrective Action Plan

As mentioned above, the licensee proposes an action plan to remedy the situation and address the deficiencies, i.e., ultimately, to reduce the risk to an acceptable level. The CNSC reviews the proposed plans as part of its compliance monitoring activities and comments on the actions and/or the schedule to ensure that the licensee has taken all reasonable precautions and measures to address the issue. Among the concerns raised by the CNSC to the licensees is the tendency not to dig deep to reach the root causes or avoiding raising questions concerning deficiencies in the human aspects

of the operation, being procedures, training and more importantly management and organizational aspects.

INCIDENT – EXAMPLE

In a licensed accelerator facility, a student was assigned the task of designing and installing circuits to measure low voltage in a radiofrequency system. While performing the work, the student received an electrical burn to his finger when attempting to measure the signal with a voltmeter on a circuit which was powered with high voltage.

Although the consequences of the incident were minimal, it was considered of important significance by both the licensee and the CNSC. Following the licensee's incident investigation report the CNSC requested a repeat of the investigation to ensure that all the generic aspects of the incident and the root causes have been identified and corrective actions are planned.

The investigations revealed a number of findings most of them of wide range impact. The first finding was that the student did not receive proper training on handling high voltage systems. Secondly, the drawings on files were not complete nor consistent with the "as-is" design. As well, the investigation determined that design review had not been performed prior to the job. The change control and work permit procedures were not followed. Finally, procedures to test any presence of high voltage did not exist. No warning labels for high voltage were present.

The licensee conducted thorough reviews of the entire practices related to high voltage and came up with several changes to prevent recurrence and improve the high voltage safety. This included establishing an authorization system to ensure that only qualified individuals in high voltage are allowed access to these systems; planning to comply with the drawing documentation requirements; issuing safety procedures for high voltage; labelling of all high voltage circuits; and developing an effective approval process for small circuits and projects. To note, in this case as in many other similar cases of incident investigations, most of the findings led to a need to enhance the quality management system, something regularly promoted by the regulator.

CONCLUSION

The CNSC considers that a systematic way of investigating incidents arising from the operation of accelerators and learning from them to improve safety is an essential capability and activity for the accelerator licensees. The CNSC promotes operating experience programs at the licensed accelerator facilities where undesirable events or near misses are turned into lesson opportunities.

ACKNOWLEDGMENTS

The author would like to acknowledge the work of Dr. Felicity Harrison, Human Performance Specialist, CNSC who played a leading role in promoting incident investigation improvements inside and outside the CNSC. Also, the author acknowledges the supporting role and valuable comments from the CNSC management particularly Mr. Henry Rabski.

REFERENCES

[1] *Nuclear Safety and Control Act*, 1997.
[2] *Class I Nuclear Facilities Regulations*, 2000.
[3] *General Nuclear Safety and Control Regulations*, 2000.
[4] Institute of Nuclear Power Operations, Human Performance Enhancement System (HPES). 1990.
[5] M. Paradies and L. Unger, TapRooT$^{@}$ Incident Investigation System, System Improvements, Inc. Knoxville, TN, 1991.