International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184 Volume 4, Number 2(April2015), pp. 27-33
© MEACSE Publications
http://www.meacse.org/ijcar

Safety Analysis for Gamma Irradiator Interlocking System

Hany Sallam and Wesam Z. Ibrahim
Operation safety & Human Factors Department
Egyptian Nuclear and Radiological Regulatory Authority, Egypt

Abstract

Beside the three well-known hazard analysis techniques, Fault Tree Analysis, Event Tree Analysis, and Hazard and Operability Analysis HAZOP, the System Theoretic Process Analysis STPA method proved to be an effective tool especially in safety analysis constraints. In STPA safety is reformulated as a control problem rather than simply a reliability or availability problem. In this paper, the STPA method is used to analyze the safety of gamma irradiator interlocking system constraints. Failure to enforce these constraints on closing and opening irradiation room could expose operators and other workers to potentially high radiation levels. Such incidents are prevented through interlocks and critical design features, and operational procedures of the irradiator. STPA method is used for analyzing the controls used in gamma irradiator to extract the safety constraints required to ensure effectiveness of the system design.

Keywords: Gamma Irradiator Interlocking, Safety Analysis, STPA.

Introduction

Like HAZOP, STPA works on a model of the system and has “ guidewords ” to assist in the analysis, but because in STAMP accidents are seen as resulting from inadequate control, the model used is a functional control diagram rather than a physical component diagram [1]. In addition, the set of guidewords is based on lack of control rather than physical parameter deviations. While engineering expertise is still required, guidance is provided for the STPA process to provide some assurance of completeness in the analysis [2].
An additional goal in the design of STPA was to provide guidance to the users in getting good results. Fault tree and event tree analysis provide little guidance to the analyst, the tree itself is simply the result of the analysis. Both the model of the system being used by the analyst and the analysis itself are only in the analyst’s head. Analyst expertise in using these techniques is crucial, and the quality of the fault or event trees that result varies greatly [3].
STPA is basically a rigorous method for examining the control loops in the safety control structure to find potential flaws and the potential for (and causes of) inadequate control [4]. STPA not only identifies the hazard scenarios identified by fault trees, event trees, and other traditional hazard analysis methods, but it also includes those factors not included or poorly handled in these traditional methods such as software requirements errors, component interaction accidents, complex human decision-making errors, inadequate coordination among multiple controllers, and management and regulatory decision making [5].

The first step in STPA is to assess the safety controls provided in the system design to determine the potential for inadequate control, leading to a hazard. The assessment of the hazard controls uses the fact that control actions can be hazardous in four ways (as noted earlier) [1],[2],[3],[4]:

1. A control action required for safety is not provided or is not followed.
2. An unsafe control action is provided that leads to a hazard.
3. A potentially safe control action is provided too late, too early, or out of sequence.
4. A safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action).

Safety Measures of Gamma Irradiator

Generally, incident prevention depends on a number of factors, the most significant of which are [6]:
(a) Safety-related control system performance, e.g. irradiator entry interlocks;
(b) Staff training and competence;
(c) The effectiveness of inspection regimes in highlighting incipient faults; and
(d) Effective preventative maintenance.

In this paper, we interested in irradiator entry interlocks analysis. Interlocks play vital role in preventing many of irradiator incidents related to human factors such as operator error, deliberate acts to undermine safety systems and responses by people to incidents also need to be considered [7]. Most irradiator incidents which have been reported world-wide have been caused, at least in part, by human factors and so it is vitally important that these issues are properly addressed. Generally, there are many examples of incidents in which human play a role in these incidents and the mitigation of these incidents:

1) Stuck source problems involving its failure to return to the storage location;
2) Fires and explosions inside irradiator chambers;
3) Source frame damage;
4) Failure of source hoist cables or transit mechanisms;
5) Irradiation chamber access problems;
6) Radioactively contaminated product;
7) Spurious alarms and interlock actuation;
8) Contamination outside the cell;
9) In the case of wet source store irradiators, storage pool liner or pipework damage; abnormal storage pool water loss; storage pool water chemistry changes and radioactive contamination of storage pool water.

Interlocking System

Human exposure to radiation is the most dangerous incident which results from radiation room accessing. To avoid such incidents a Safety Related Control System (SRCS) needs to have two features [6]: it should make it impossible for a person to gain access to the irradiator source when in the exposed position, and it should be fault tolerant. Engineered exposure control is achieved by interlocking source mechanisms with the points of entry to the exposure chamber so that they remain locked while the source is exposed as shown in Fig.1, For example, this can be achieved by having a mechanical device at irradiator entrance doors or lids which directly disables the source exposure mechanism. Interlocking can also be achieved by an electrical ‘logic’ system which makes decisions about irradiator status from the inputs received from control devices such as source rack position detectors, door closure detectors and in-cell radiation detectors.

Electrical techniques are more flexible than mechanical designs and are often preferred by designers and manufacturers nowadays. But they can be more difficult to make fail-safe than mechanical safety interlocks. With the advent of software-driven programmable controllers such as PLC, the issue of fault tolerance and mitigation in the SRCS has become vitally important to overall safety assurance [8] [9].

Door closure switches designed and installed so that when they fail, following return spring failure or poor electrical connection for example, the source exposure mechanism remains disabled [10] [11].

Most systems allow interlocks to be disabled so that some types of maintenance can be completed and so that emergencies can be dealt with, but such actions should be very strictly supervised and preferably subject to a permit-to-work system.

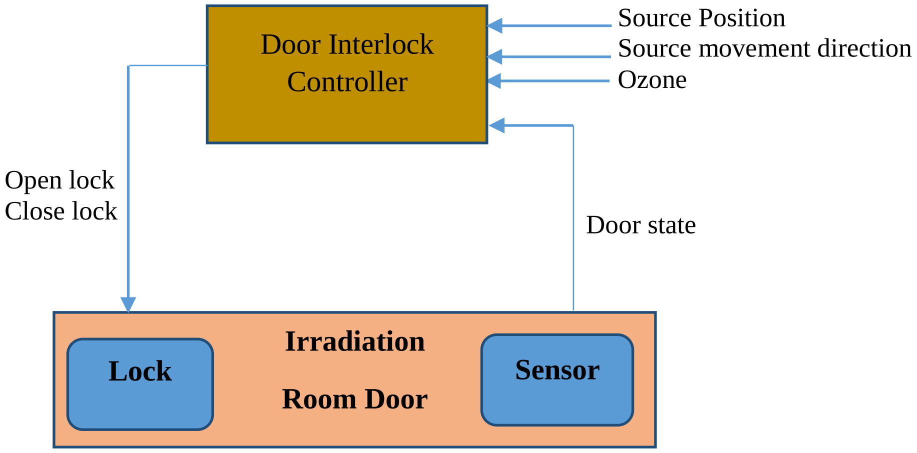

Fig.1, Door Interlock Control System

Entry to irradiation area

Entry to the irradiation area is possible only by permit of plant operator, and by the following conditions:

- There is no radiation hazard in the irradiation area
- Source are in the storage position

In this case, the operator should initiate entry process carrying out the following steps:

- Set entry mode on computer.
- Waite until ozone delay time passed.
- Take off master key from control panel, this operation starts counting delay time.
- Control of the workable condition of the radiation-detection device (fixed to the masterkey) by test source at the door of the personnel maze.
- Open the door by master key. The lock gives signal to the magnetic clutch to open the door.
- Take out the master key from the lock.
- Take out the safety chain from its lock.
- Activate entry to radiation room before the security time elapsed.
- In the case of fulfillment of the above program the entry is considered successful, the operator stay in the irradiation room.

The control system prevents entry in the following cases by keeping the magnetic lock of the radiation room door closed [10], [11], and [12]:

- Irradiator is not stopped by normal or emergency stop.
- Delay time for exhausting the ozone is still on.

Applying STPA Gamma Radiator Interlocking

There are many parameters controlling the operation of opening or closing the irradiation room door. The most important one is the source position, whether in radiation position or in storage position and the ozone decay time, finished or not. Other parameters related the opening the door such as the door status, the source movement direction, there is an emergency or not, and whether there is a personal in the radiation room or not. These parameters and their status are shown in Fig. 2.

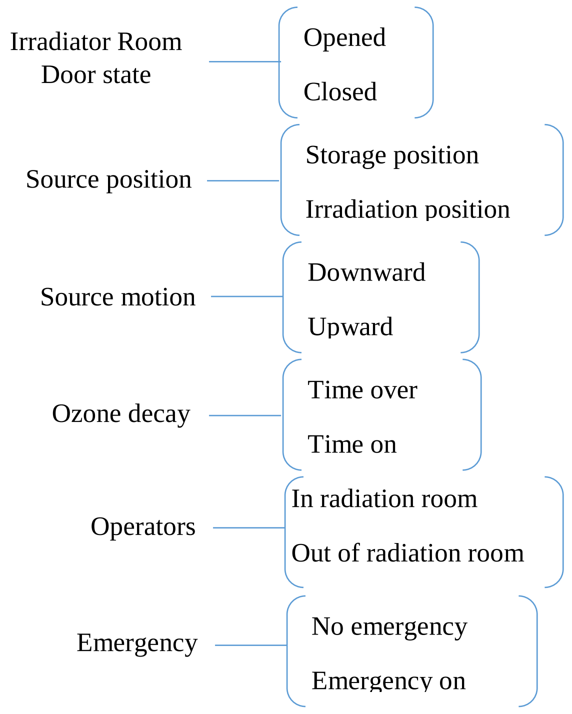

Fig.2, Process model for Gamma Irradiator

Based on these parameters, the target of this hazard analysis is to avoid human error such as opening the irradiation room door while the source is in exposure position or closing the door and starting moving the source from storage position up to the exposure position while still there is personal in the radiation room. Another error is to open the door while the source is moving up or down which means there is a possibility of operator exposure to radiation since the source is not fully shielded under the water in storage position. Also, ozone is still exist in the radiation room or decayed is important parameter in deciding opening the door or not. Ozone inhalation causes harmful health consequences. When inhaled, ozone can damage the lungs. Relatively low amounts can cause chest pain, coughing, shortness of breath and throat irritation. Ozone may also worsen chronic respiratory diseases such as asthma and compromise the ability of the body to fight respiratory infections [13].

For the radiation room door interlock case, four hazardous types of behavior are considered:

1. A power off command (the source is moved down to storage position) is not given when the door is opened, or
2. The door is opened and the controller waits too long to turn the power off the source (moving down to storage position);
3. A power on command (the source is moving up to radiation position) is given while the door is open, and
4. A power on command is provided too early, (when the door has not yet fully closed).

STPA method starts by selecting a control action and construct a context table [1], [2] as shown in Table 1. The first column indicates that this table analyzes the control action Door Open the next four columns correspond to the process model variables for the selected control action. Each row is populated with a unique combination of process model values. Each row is then evaluated to determine whether the control action is hazardous in that context, and the result is recorded in the column on the right with yes (i.e. hazardous) or no (i.e. not hazardous).

For example, providing an open door command in the context of the source be in storage position, there is no ozone, and whatever there is an emergency or not is not hazardous.

Table 2, shows a similar table for the type not provided. Each hazardous row (row with a "yes" in the right column) in either tables is an unsafe control action that can be recorded in a summary table similar to Table 3.

Table 1,Context Table for "Control Action is given"

Control Action	Context State				Hazardous
	Source position	Source motion direction	Ozone	emergency	If CA provided any time in the context
Door commanded to open	radiation position	Doesn't matter	Exist	No emergency	Yes
	radiation position	Doesn't matter	Exist	Emergency	Yes
	storage position	Doesn't matter	Exist	No emergency	Yes
	Storage position	Doesn't matter	Not exist	No emergency	No
	Storage position	Doesn't matter	Exist	Emergency	yes
	Storage position	Doesn't matter	Not exist	Emergency	No
	Doesn't matter	Moving up	Not exist	Emergency	Yes
	Doesn't matter	Moving up	Not exist	No emergency	Yes
	Doesn't matter	Moving down	Exist	Emergency	Yes
	Doesn't matter	Moving down	Not exist	Emergency	Yes
	Doesn't matter	Moving down	Exist	No emergency	Yes
	Doesn't matter	Moving down	Not exist	No emergency	Yes

Table 2,Context Table for "Control Action is not given"

Control Action	Context State				Hazardous
	Source position	Source motion direction	Ozone	Emergency	If CA not provided any time in the context
Door not commanded to open	Radiation position	Doesn't matter	Exist	No emergency	No
	Radiation position	Doesn't matter	Exist	Emergency	No
	Storage position	Doesn't matter	Exist	No emergency	No
	Storage position	Doesn't matter	Not exist	No Emergency	No
	Storage position	Doesn't matter	Exist	Emergency	No
	Storage position	Doesn't matter	Not exist	Emergency	Yes
	Doesn't matter	Moving up	Not exist	Emergency	No
	Doesn't matter	Moving up	Not exist	No emergency	No
	Doesn't matter	Moving down	Exist	Emergency	No
	Doesn't matter	Moving down	Not exist	Emergency	No
	Doesn't matter	Moving down	Exist	No emergency	No
	Doesn't matter	Moving down	Not exist	No emergency	No

Table 3, Unsafe Control Action for Irradiation Room Door

Control Action	**Not provided causes hazard**	**Provided causes hazards**
Open door	UCA1: door not commanded to open for emergency while the source is in storage position and ozone not exist	UCA2: door commanded to open while the source in radiation position UCA3: door command to open while the ozone exist in the room. UCA4: door is commanded while the is moving up or down

Results

Based on Table 3, the identified hazardous behaviors can now be translated into safety constraints (requirements) on the system component behavior. For this case, four constraints must be enforced by the power controller interlock:

1. The source must always be in storage position when the door is open;
2. If the door is opened, the source must move down to storage position.
3. Moving up the source command must never be issued when the door is open;
4. Starting the irradiator command, must never be issued until the door is closed and no one in radiation room.
5. At any case whatever in normal operation or emergency, opening the door must never be issued until the source is in storage position and the ozone is decayed.
6. The door must never be commanded to open until the ozone is decayed after the source is moved to storage position.

These requirements shall be fulfilled in the design of the control system of the irradiator beside the operating procedures that the operator shall follow in normal operation and emergency cases for entering the radiation room.

Conclusion

In this paper, the safety analysis techniques STPA is used to analysis to the control system of the gamma irradiator interlock of the irradiation room. STPA method proved to be an effective tool in safety analysis especially in safety requirements analysis. The results of analysis extracted to set of constraints or requirements to ensure the safety of operator and workers in the gamma irritator facility. The interlocking system must ensure the radiation room door is closed before the exposure of the source,the door shall not open until the source is returned to full shielded position and ozone is exhausted. STPA can be used for more analysis to get the causal factors, and this will be our future work.

References

[1] Thomas, J., F. Lemos, and N. Leveson, Evaluating the Safety of Digital Instrumentation and Control in Nuclear Power Plants, in NRC Technical Research Report 2013.

[2] Nancy G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety Engineering Systems, Jan 13, 2012.

[3] Thomas, J., and N. Leveson, Performing Hazard Analysis on Complex Software and Human Intensive Systems, in International System Safety Conference 2011, System Safety Society> Las Vegas, NV.

[4] Cody H. Fleming, M. Seth Placke, and Nancy G. Leveson, STPA Analysis of NextGen Interval Management Components: Ground Interval Management (GIM) and Flight Deck Interval Management (FIM), MIT Technical Report July2014.

[5] Leveson, N.G. A New Approach to Hazard Analysis for Complex Systems. International Conference of the System Safety Society, Ottawa, August 2003.

[6] Health and Safety Executivehse, Safety in The Design and Use of Gamma and Electron Irradiator Facilities, HSG94 Second edition 1998.

[7] Health and Safety Executive HSE, Reducing Error and Influencing Behavior, HSG48 Second edition 1998.

[8] SeoRyong Koo, Poong-hyunSeong, and Sung Deok Cha, Software Design Specification and Analysis Technique for the Safety Critical Software Based on Programmable Logic Controller (PLC), in High-Assurance Systems - HASE Conference , pp. 283-284, 2004.

[9] International Atomic Energy Agency, Radiation safety of gamma and electron irradiation facilities, Safety Series No. 107, IAEA, Vienna (1992).

[10] International Atomic Energy Agency, Manual on panoramic gamma irradiators (Categories II and IV), IAEA-PRSM-8, IAEA, Vienna (1996).

[11] American National Standards Institute, Safe design and use of panoramic, wet source storage irradiators (Category IV), ANSI-N43.10-1984, New York (2001).

[12] Atomic Energy Licensing Board, Lembaga Perlesenan Tenaga Atom, Code of Practice on Radiation Protection Of Nonmedical Gamma & Electron Irradiation Facilities, LEM/TEK/57, 02 December 2008.

[13] Waring MS, Siegel JA. The effect of an ion generator on indoor air quality in a residential room. International Journal of Indoor Environment and Health,Volume 21, Issue 4, pages 267–276, August 2011

.