System safety theory and human factors approach to patient safety for radiotherapy

Seraphin Chally Abou

Mechanical and Industrial Engineering Department; Environmental Health and Safety Program
University of Minnesota Duluth; 1305 Ordean Court, Duluth, MN 55812; Email*: sabou@d.umn.edu*

Abstract

The research questions in this study while developing modern medical technology for safer applications of radiation therapy are – what medical and radiobiological effects and their quantitative models must be taken into account while defining the radiation risk. The uncertainty in the expression of these consequences for the delayed effects is one of the important problems the solution of which is necessary for radiation safety. The main principles of ensuring the radiation safety and the assessment of software technological risk developed on the basis of the intrinsic compatibility with safety systems theory, as an example, those which follow the concept of "*Inherent safety*" are presented in this paper.

Keywords: Safety-critical system; Health risks; Ionizing radiation; Dosimetry; Software risk

1. Introduction

In medical uses of radiation, ionizing radiation has two different uses – for diagnosis and for therapy. Both are intended to benefit patients and, as with any use of radiation, the benefit must be outweigh the risk. The foundation of radiation oncology is based on the interaction between matter and energy, [8]. Considerable attention is typically given to radiation safety in the design of irradiators and initially establishing the program. However, one component that may not receive enough attention is applying the continuous improvement philosophy to the radiation safety program. The nuclear field, both industry and medicine have been dealing with the controversy of the dose level of ionizing radiation for many decades. One can argue that the optimization approach, to keep the effective doses As-Low-As-Reasonably-Achievable (ALARA), taking economic and social factors into account (ALARA) principle, which is beyond a precautionary approach. The late health effects of exposure to low doses of ionizing radiation are subject to scientific controversy. While one view finds threats of high cancer incidence exaggerated, the other view thinks the effects are underestimated. However, because of these stochastic effects, no scientific proof can be provided.

New tendencies for using human factors and systems engineering methods and principles to solve patient safety problems are accepted in science and engineering community, since the publication of "*To Err is Human: Building a Safer Health System"*, [8]. However, no adherence to systems theory approach leads to lacks of understanding of human factors and systems engineering, and confusion remains about what it means to apply their principles, [9]. Ideally, hazard analysis should precede or at least accompany system design in order to avoid the problems associated with changing design decisions after they have been made. The problem is that most of the existing hazard analysis techniques require a detailed design before they can be applied, because they rely on identifying potential component failures and their impact on system hazards.

The development of the design and the hazard analysis can go hand-in-hand, starting with the requirements for control of the high-level hazards and then refinement of the design decision making. These concepts characterize those safety-critical systems in which the insertion of the emergency systems is based on physical laws without using active components affected by reliability problems. The wide use of natural convection is an outstanding example of this new kind of approach. The radiation therapy systems and radiobiological effects management becomes consequently more reliable and safer when the technological innovations, software and others safety attributes are well balanced. Therefore, achieving safety requirements is a balancing act – but the balancing must be done as part of the developing process, for the goal should be to prevent accidents in the first place or at least to make them sufficiently improbable that the risk is acceptable.

However, since safety is a property of the system, this balancing act creates difficulties with determining the boundaries of the scope. For example, it is obviously desirable for software engineers to participate in the design of the system architecture, since it is that which identifies safety-critical components in an overall design and generates the requirement for high-integrity software. It is also absolutely necessary for change control and problem resolution to be system-wide so that the system design can change in response to necessary software change. Therefore, this paper explores how ALARA and high-integrity software principles are influential in the radiation therapy systems. It uses systematic method to analyze, control and evaluate the radiation safety issues of medical exposures. It is viewed as a more rational approach of the design of operational safety in order to evaluate inherent safety potential related to: Software, hardware, and the policy that controls all phases of the process design. Moreover, this policy is defined as hazard identification and safety insurance control that includes several principles: definitions and requirements, hazard identification, safety insurance control, safety critical limits, monitoring and control, software verification and validation of the accuracy in the delivery the treatment, system log and documentation.

2. Hazard identification and safety insurance control

A process involving a combination of technical, personal, behavioral, environmental and work process factors can cause safety problems for medical uses of radiation. Human error is one aspect, such as wrong instructions or manipulation, and uncertainty in quantitative analysis. System error is another important aspect, which can also be divided into four categories: pure hardware, pure software, hardware triggered by software, and software triggered by hardware.

Nevertheless, in attempt to systematically assess irradiation process and also to determine what is to be covered while regulatory compliance audits are a component of this process, the most useful evaluation will extend beyond looking only at compliance and determine whether the radiation safety program is the most appropriate for the particular application. Several aspects of the irradiator operation, not all of which may routinely be considered “radiation safety”, per se, should be included: Design aspects of the irradiator and operating system, system controls, and maintenance procedures, as well as the more traditional radiation safety program components such as surveys, measurements, training, and dosimetric comparison between static and dynamically shaped beam deliveries.

It is agreed that the safety of any medical device system is dependent on the application of a disciplined, well-defined, risk management process throughout the product life cycle, [5], [6]. Hardware, software, human, and environmental interactions must be assessed in terms of intended use, risk, and cost/benefit criteria. Therefore we addressed these issues in the context of

medical devices that incorporate software. The principles of risk management are elaborated from the domain of software engineering perspectives.

For the uses of radiation in diagnostic medicine and radiotherapy, successful radiation management and technological methods requires cooperation among the various groups with relevant responsibilities if the desired exposure goals are to be achieved. Before discussing systems engineering, it is first necessary to develop an understating of systems. A system is a set of components that interact to accomplish a common goal. In a healthcare context, the ultimate goal is to provide safe, high-quality patient care. However, a healthcare delivery system has many other goals that need to be simultaneously addressed. Some of those other goals include supporting employee performance, addressing business needs such as profitability and positive image, and meeting external environment needs such as radiologist's safety. If a healthcare delivery system is not been designed to address all of these goals, then the long-term likelihood of delivering safe, high-quality care diminishes.

Systematic hazard identification and safety insurance control strive to enhance process safety by introducing fundamentally safer characteristics into process design. In this sense, we define the inherent safety implementation by a set of procedures of selecting and designing a process to eliminate hazards, rather than accepting the hazards and implementing add-on systems to control them. Therefore, inherently safer medical uses of radiation have less "*built-in*" hazard potential than systems utilizing ionizing radiation with a conventional process concept. In order to achieve that result throughout the development phases of hardware and software engineering process, and conceptual design, major decisions on process principles is essential to support hazard management. Moreover, the systems engineering activities would include the monitoring and coordination of the hardware and software development activities, and dosimetric efficiency analysis for different beam delivery mechanisms (e.g., statically, and dynamically shaped).

In hazard identification process, the concept of causality is of high importance, since interactions between components are considered. Therefore, the preliminary design phases offer the opportunities of implementing the inherent safety principles, preliminary hazard analysis, radiation dose reporting and management approaches in combination with chemotherapy including radiation field reduction, health physics planning, exposure control during job execution, implementation of a radiation protection culture, and software technological risk analysis. Each of these entities and their specificity contribute to the risks and the uncertainties at the system level individually and collectively. The complexity of the relationships, interactions, and constraints that individual elements and artifacts have to each other presents a number of safety concerns. Iterative safety-driven design process is illustrated in Fig.1.

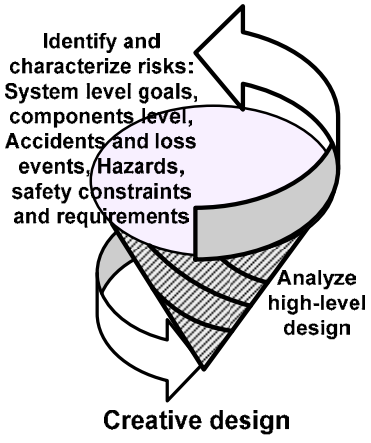

Fig.1 Safety-driven design process

For example, consider the translation of a patient underneath the radiation. If the radiation beam stops unexpectedly, the moving bed must stop immediately if the treatment is to be restarted at the correct location since matching the start and stop would not otherwise be possible. Similarly, if the bed stops moving, the radiation beam must also stop immediately or the patient would receive a high dose of radiation to a very isolated location. The speed of the bed must also be monitored very closely since it plays a major role in determining the local or spatial distribution of the effective dose the patient receives. The faster the patient is translated, the lesser the dose he/she receive.

As a result, the reliability and safety characteristics should be evaluated systematically as early as possible in the system design process. However, the evaluation of inherent safety in the early design phases is a challenge, since the lack of detailed information complicates safety evaluation and decision-making. At that time, much of the detailed information-on which the decisions should be based-is still missing, because the process is not designed yet. On the other hand, once the process is designed in detail, there would be all the information, but not the freedom to make conceptual changes. This paradox makes it necessary to implement a dedicated methodology for evaluating inherent safety in conceptual design of medical uses of radiation to allow early adoption of its principles and the technological risks associated with it (a realm of decision making under “uncertainty” and “risk”).

It is difficult if not impossible to perform experimental analyses of hazard analysis techniques in modern safety engineering due to the scarcity of accidents [3]. It is possible, however, to compare the scenarios generated by the analyses. The following sections provide the assessment and management of risk principles that can ultimately enable any organization involved in safety-critical software development to meet safety-driven design for software-intensive radiation therapy quality and performance goals while controlling costs and schedule.

3. Assessment of software technical risk

Usually, the hazard log is used at system level to capture different types of information such as the hazard severity and type of potential loss resulting from the hazard. However, risk control strategies that use the control loops and the control flaw taxonomy to find control flaws in systems are by no means complete. The identification of risk with expectation value requires that the severity of outcomes can be measured in numerical terms. Ideally such a measure should refer to over-all utility, in which case risk analysis becomes a branch of expected utility theory, [12]. Though, this approach may be regarded as dual to the model with stochastic dominance constraints with respect to a random benchmark. In that case, if the process model been used for the control is wrong from the beginning, there may be missing or incorrect feedback to update the model as the process changes, the updating algorithm may be incorrect, or the control algorithm may not properly account for time lags in the control loop. The result may be uncontrolled disturbances, unhandled process states, inadvertent commanding of the system into a hazardous state or unhandled or incorrectly handled system component failures. Note that this theory interprets component failure as a causal factor in accidents and accounts for the system reliability, but it is only one aspect of causality when we are dealing with safety-critical systems.

This study is to demonstrate that an equivalent formulation of the stochastic dominance constraint leads in a similar way to rank dependent expected utility theory. In this way, the proposed model in this study provides a link between these two competing economic theories, assuming that not all dangers come with probabilities assigned to them. Moreover, the terms

"*risk*" and "*uncertainty*" are used to distinguish between those events that do and those that do not come with quantifiable probabilities, as known in decision theory, [4]. Figure 2 depicts an example of standard system control structure for a computer control radiotherapy system. In the example (and in current standard computer controlled conformal radiotherapy system architectures), interactions between functional elements are controlled by the scanhead command and data handling functional element. The control structure can be evolved iteratively to capture departmental network and lower-level interactions. Also, it may be used to inform the lower-level design as will be discussed later in the paper.

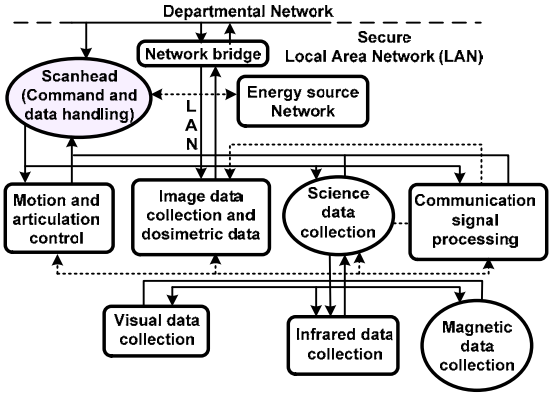

Fig.2 Control structure

The sequence processor handles one of the most important treatment delivery tasks: the sequencing of events used for patient setup, treatment simulation, and treatment delivery, and capture of treatment delivery data. Since this structure is different from the conventional treatment delivery system involving a limited number of treatment ports (where most of the steps used for patient and machine setup and data recording are handled by human operators), there are many issues to be considered when moving from the conventional treatment delivery scenario to a more automated method. Key issues are safety and efficiency.

A number of models exist which attempt to estimate delivered errors in software. A particularly fruitful area of research developed in recent years is the application of reliability theory to software fault phenomenon. Useful as reliability concepts may be, they tend to describe the aggregate behavior of software over time and do not attempt to relate the failure process to management or engineering intervention. Specifically, how does one use the probabilistic nature of software failures in choosing a fault correction plan?

Four major internal and external forces, which operate in the environment of software development, are identified in this study: the organizational safety culture perspective and nature, the software powershift paradigm-the shift in functionality and in decision making from hardware to software engineers, technological innovation and know-how, and other forces, such as the social/behavior performance. Moreover, the software development activity itself is characterized by five major traits: the management of change, the protection against organizational failure, the maturity of the development process, design and technological capability, and technological know-how. Influenced and driven by the internal and external environment, these five traits generate software risks of two types: *technical risk and non-technical risk*. To assess and control these risks, a holistic framework based on hierarchical holographic modeling relevant to information modules of radiotherapy is adopted in this study.

4. Conceptual framework

A good first way to apply systems engineering principles for healthcare safety is to develop in-depth understanding about the system and to learn to analyze the system. Analyzing a system is an important first step in planning changes, implementing technology, or conducting safety analyses. The outcome of a systems analysis is typically a graphic map depicting the inputs, transformations, and outputs of the system under study. These are drawn as flowcharts showing how the various processes and steps within processes in the system interact. A work system analysis can help identify problems in current processes, it can be used as a proactive approach to designing new systems with fewer hazards, and it can be used in research to help understand why problems exist within the patient care process.

For the control structure shown in Fig.2, except for the sharing of the accelerator control functions (there is only one accelerator), the two control system processes are independent. Each connection involves establishing two communication channels that are distinguished as synchronous and asynchronous. Commands are sent from the sequence processor (SP) to the control computer using the synchronous channel and the control computer replies on this same channel immediately after accepting the command. Moreover, the control computer performs checks on the validity of a command and generally replies with an acknowledgment or an error code. The asynchronous channel is used only by the control computer for reporting high priority events such as a beam off report or a status change report. The main control system of these accelerators provides a serial interface that allows access to the current geometry, dosimetry, and status parameters for the machine, provides the ability to enable/disable the beam, and has the ability to set up some of the geometry parameters. All of these functions are relatively normal features required by a standard "*Record and Verify*" (R/V) system. Additional safety actions to perform are to define the hazardous states in the system that would allow accidents to occur. These hazards are then translated into safety constraints on system state and behavior so that the hazardous states cannot occur.

5. A framework for considering human factors

When people are involved in systems and controls, the process is often referred to as socio-technical systems engineering. Systems engineering refers to the design of the overall system. The focus is on effectively designing and integrating the components of a system proactively, instead of building the components separately and trying to fit them together later. Socio-technical systems engineering is a systems engineering method focused on designing the social aspects of the system (which consists of the people in the system, such as the healthcare professionals and patients, and all that is human about their presence, such as their knowledge and skills) and the technical aspect (i.e., tools, techniques, technology, procedures) to work together effectively. The basic science of socio-technical systems engineering is known as human factors engineering.

Mathematical models and paradigms have become the quintessential instruments in achieving efficiency, effectiveness, reliability, and high-quality products that meet consumer demands. Some of these models are mathematical, analytic, conceptual, or behavioral. For example, the Japanese made extensive use of behavioral models such as the continuous improvement advanced in *Kuizen*, [7]. To implement these models, namely, to translate the mathematical logic and optimization inherent in these models into correct and representative operating rules, software engineers must have an understanding of the models. In software-intensive systems, hardware engineers typically are not required to have this knowledge, although there are instances where hardware engineers do contribute significantly to the translation of these models

and continue to exert major influence over the entire system (an example is those who design integrated circuits).

Another tool for understanding systems engineering concepts is the systems engineering initiative for patient safety model of work system and patient safety. These systems engineering conceptual framework is targeted at those interested in applying systems engineering ideas for patient safety goals. The assessment and management of both types of risk involved in the life cycle of software development (i.e., software technical risk, and software non-technical risk) include the following:

- Identification, measurement, analysis, and evaluation of risk through: (1) the four sources of risk: human, organizational, hardware and software; (2) the temporal domain of software development, and (3) the functional perspective with its attributes: requirement, product, process, people, management, environment, and development system
- Development of strategies and their associated trade-offs, and
- Communication of risk

This approach categorizes interactions between the person and the system and then identifies where these interactions can be improved. The risks of not meeting system safety and performance, cost, and schedule can be successfully identified, quantified and measured, evaluated, and managed only when a systemic and holistic process of assessment and management is employed. Depending on the forces exerted and on the software development practice itself two types of risks are likely to emerge-software technical and non-technical risks. Indigenous to these forces is the powershift from hardware to software; consequently, such change must be recognized and managed.

Conclusion

This paper is grounded on the premise that change, such as the organizational behavior, human factors, and powershift from hardware to software, necessarily introduces new sources of risk. Software risk management must confront a host of new organizational uncertainties, including new working patterns and responsibilities, and new people. Indeed, managing change is a first, albeit a critical step in confronting these new sources of risk. Thus, managing change is an imperative prerequisite to managing risk. Healthcare's past remedy to the lack of patient safety, blaming individuals, has not solved safety problem. Thus, alternative approaches are needed. One approach that has worked in other industries is to use the principles and methods of systems and human factors engineering. The systems approaches explained in this paper can relieve in designing safer and more efficient systems.

Reference

[1.] Chrissis M.B., Konrad M., and Shrum S., Capability Maturity Model Integration (CMMI), USA: Addison-Wesley, 2005

[2.] Dayhoff R.E., Kuzmak P.M., and Meldrum K., "Integrated Multimedia Patient Record Systems," in Biomedical Information Technology, D. D. Feng, Eds. USA: Elsevier, pp.343-357, 2008

[3.] Dehlinger J. and Lutz R.R. "Software fault tree analysis for product lines"; 8th IEEE Symposium on High Assurance Systems Engineering (HASE '04), Tamp, FL, pp.12–21, 2004

[4.] Green J. and Jullien B., ''Ordinal Independence in Nonlinear Utility Theory''; Journal of Risk and Uncertainty, vol.1, pp.355–387, 1988

[5.] IAEA, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna 1996

[6.] IAEA, Radiation Protection and the Safety of Radiation Sources (Safety Fundamentals), Safety Series No. 120, IAEA, Vienna 1996

[7.] Imai M., *Kaizen.* New York McGraw-Hill, 1986
[8.] Institute of Medicine, "To err is human: Building a safer health system"; National Academy Press; Washington DC, 2000
[9.] Kulpa M.K. and Johnson K.A., Interpreting the Capability Maturity Model Integration (CMMI), 2nd ed., USA: CRC Press, 2008
[10.] Pope, R.E., The Bayesian Approach: Irreconcilable with Expected Utility Theory?, in B. Munier (ed.), *Risk, Decision and Rationality*, Reidel, Dordrecht, pp.221–230, 1988a
[11.] Samuelson P. "Probability, Utility and the Independence Axiom", *Econometrica, vol.*.20, pp. 670–678, 1952
[12.] Von Neumann J. and Morgenstern O. "Theory of Games and Economic Behavior"; Princeton University Press, Princeton, 1947