BEST PRACTICES IN DESIGN & DELIVERY OF A NEW TRITIUM FACILITY

I Bonnett[1], A Busigin[2] and A Griffiths[3]
[1] Light Isotope Technology Centre of Excellence, GE Hitachi Nuclear Energy Canada Inc., Peterborough, Ontario, Canada
[2] Special Separations Applications, Inc. Brockville, Ontario, Canada
[3] GE Healthcare, Maynard Centre, Cardiff, UK

Abstract

Tritium is of particular interest to the Canadian nuclear industry given that it is in the nature of CANDU® reactors to build up high levels of tritium over time.

Since the last major Canadian tritium facility was built, expectations of best practice and ALARA (As Low As Reasonably Achievable) have developed, including incorporation of international safety standards such as IEC61508, adoption of safety hierarchy concepts in risk reduction, the use of modern day technology and demonstrable requirements traceability techniques.

The paper outlines best practices adopted and developed further by GE* in its design and delivery processes for tritium facilities.

1. Introduction

Tritium is of particular interest to the Canadian nuclear industry given that it is in the nature of CANDU® reactors to build up high levels of tritium over time.

The characteristics of tritium and its compounds represent a significant challenge in the design and operation of high inventory tritium facilities. Some of these engineering challenges include:

- dispersion due to its high diffusivity and its ability to isotopically exchange with protium
- containment due to its ability to permeate through most materials of construction
- difficulty in tracking and monitoring due to its weak beta radiation
- hazards arising from its flammability in elemental form and radiotoxicity especially in the water form

There is very little regulatory direction given in prescriptive nuclear regulatory framework jurisdictions, such as the United States, for high inventory tritium processing facilities mainly due to the small number and diverse nature of these facilities. Some government organizations

* In this paper GE refers to both GE Healthcare and GE Hitachi Nuclear Energy Canada Inc.

have attempted to provide tritium guidelines [1]; however, they tend to be specific in nature and strongly influenced by the type of operation conducted in their facilities.

Since the last major Canadian tritium facility was built, expectations of best practice and ALARA have developed further, including incorporation of international safety standards such as IEC61508, adoption of safety hierarchy concepts in risk reduction, the use of modern day technology and demonstrable requirements traceability techniques.

This paper outlines best practices adopted and developed further by GE in its design and delivery processes for tritium facilities based upon practices used in the delivery of the Tritium Waste Treatment & Enrichment Facility [2] and current methods used in reactor service work for existing CANDU® power stations.

2. Management Arrangements and Overview

The quality assurance/management system arrangements for projects that deliver tritium facilities should be the planned, systematic and integrated series of performance, verification, assessment and review activities undertaken to assure the quality of the facility and its systems.

The totality of these arrangements should provide confidence that a new tritium facility will perform according to its requirements, from the time it is declared in-service, to the time it is permanently removed from service.

GE has adopted the principles of the Project Management Institute [3] to ensure effective overall management of projects, shown in Figure 1, with major activities interrelated through timeline, verification and validation.

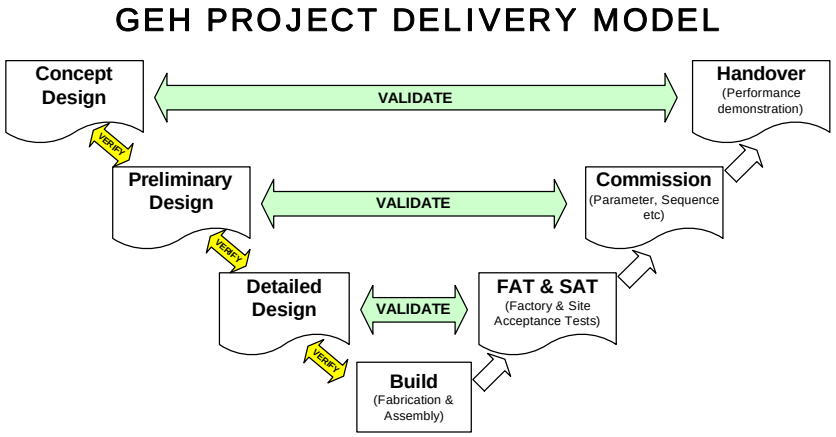

Figure 1: GE's Overall Project Delivery Model for new Tritium Facilities

3. Design Principles

Formal Design Principles have been used as a method to ensure that new facilities are designed and delivered meeting all customer and legal requirements and expectations.

A facility designed following well established Design Principles would meet and exceed regulatory expectations such as the Safety Assessment Principles from the UK's Nuclear Installation Inspectorate [4] if the nuclear facility was built in the UK, and wider international safety principles of the IAEA [5].

GE's Design Principles are essentially fundamental overarching statements encompassing all considerations for the design of a new facility. These are the starting points, in conjunction with the User Requirements Specification (URS) for a project.

Design Criteria are developed and provide further detail to aid GE to substantiate the design. They encompass criteria that reflect working practices at particular operating sites and can be particular to individual projects focussing on the specific requirements of that project.

As the tritium facility design develops, design concepts are tested during GE's design reviews against the Design Criteria, and where necessary, by the Design Principles. To illustrate this concept, the following is a Design Principle related to managing flammable and explosion hazards:

- The design shall minimise the *hazards* from explosion and inflammable, toxic and asphyxiating gases.

This Design Principle is implemented through a GE Quality Engineering Procedure that sets out detailed Design Criteria as illustrated by the following examples:

- The Hazardous Area Classification Approach shall follow the standard approaches found in IP Part 15 [6] where not directed through GE's Quality Engineering Program.
- All point source zone radii for continuous, primary and secondary release will be determined through calculation and not estimated through standardised hazard radii found in Chapter 5 IP Part 15. This is because the standard radii provided do not relate to the scale of operations and, due to the scale of operations, electrical equipment suitable for zoned areas may not be practicable and zoned radii should be minimised or completely removed. Point source leaks will apply the leak hole diameters found in GE's Quality Engineering Procedure for determining zone hazard radii.

"Design" in the context of the following Design Principles implicitly means design for the lifecycle of the plant including installation, commissioning, operation and decommissioning.

4. User Requirement Specification

The User Requirement Specification (URS) is a high-level reference document generated by the customer (the end user) that introduces the facility requirements, associated functions and overall objectives. It is an important document used in conjunction with Design Principles to produce the design.

The URS should contain specific tangible requirements including:

- The overall objectives of the project
- The functional and performance requirements such as throughput and overall efficiency

- The specific constraints placed by the customer on the design e.g. waste form limitations
- Specific safety and environmental requirements such as dose limits and objectives, emission targets, etc
- The inputs and outputs for the facility such as feed stock quality, product quality, etc
- The environmental operational conditions and limits to which the facility and systems will be designed
- Overall bounding of the project/facility limits by defining interface points

Often the project team helps to write the URS with the customer, which has the benefit of ensuring that the project team fully understands the ultimate customer requirements, and that the customer fully understands the project team's approach, which may include requirements critical to the design that the customer may have not considered. Establishment of the URS is key to the overall delivery and final validation of the facility.

5. Design Process Overview

A successful Design Process ensures that the facility and its systems are designed in a systematic and rigorous manner to reduce risk (safety, environmental or business) while taking into account all stakeholder requirements and meeting best practice.

The importance of getting the design right has been proven time and time again, from a safety aspect, poor selection of technology and failure to provide adequate protection systems have had dramatic consequences, while from cost control aspect an established rule of thumb that has been well documented states correcting design flaws in the field has been proven to be 100 times more expensive than correcting the flaws during the design phase [7].

A well thought-out and structured design process can bring many advantages besides avoiding safety and cost overrun risks. These benefits include:

- More accurate project planning and estimating
- Simplification of ALARA (As Low As Reasonably Achievable) and Best Practice justification in safety cases
- Consistency in design leads to standardization, bringing benefits of bulk cost reductions and minimizing spares holding during operation
- Formalized and structured requirement definition allows for systematic verification and validation processes, meaning impact of changes and understanding of design intent is more effective and transparent

The Design Process adopted by GE for design and delivery of tritium facilities is built upon a proven quality system that has been able to provide these benefits.

5.1 Concept Design

In GE's project delivery model a comprehensive suite of optioneering studies is performed during the Concept Design phase using a formalised Quality Engineering Procedure.

The process builds up the selection of options in a logical and systematic way ensuring that consideration of all relevant Design Principles and URS requirements is performed. In this stage of the process, the aim is to promote inherent low risk designs that minimise the safety, environmental and business risks during the earliest part of the project. Examples of these are low inventory processes, simple continuous plant, proven technology etc. This early design stage is crucial in maximizing the inherent safety[8] within the process as illustrated in the Figure 2. Hence, already the demonstration of meeting wider considerations such as the ALARA principles can be shown at this early stage of the project.

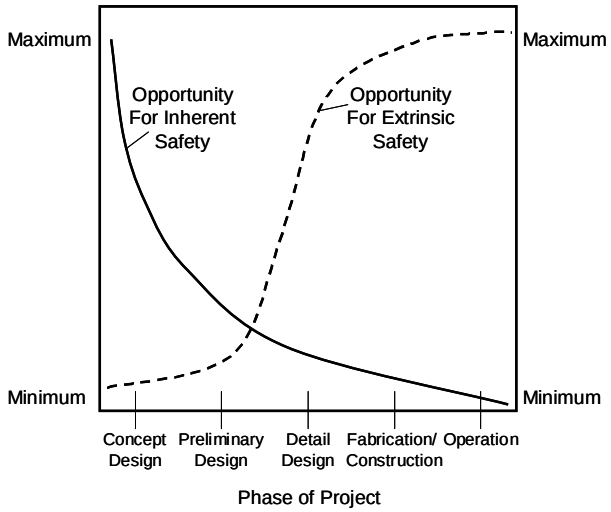

Figure 2: Effects of timing on Design Changes
(figure reproduced and modified based on illustration from reference 7)

When all options have been recorded, the most obvious contenders are streamlined for further detailed evaluation. This is carried out by:

- Ensuring that all the functional and performance requirements are met by the selected options
- Comparing the options against the topic criteria used in the evaluation step (note that this is superficial at this point and topics are used as headings for discussion only)
- Streamlining down to 3 or less options and recording the reasons for de-selection

Key to the GE option study process is the idea that at least two candidate solutions should be presented and analysed. There is a strong tendency for some engineers to pre-judge and automatically select one technology above all others and by-pass this important process. By considering at least one other option a comparison activity is performed which can highlight both the strengths and weaknesses of both options, including the strongly favoured one. This early identification of the weaknesses of a preferred technology is often missed, meaning that projects discover drawbacks at later stage, incurring delays or cost overruns.

The comparative GE analysis activity ensures that the design team considers each option against the wider lifecycle aspects including technology risk, delivery and operating cost, constructability, waste generation, inherent safety, operator activities, spatial requirements, decommissioning, etc.

Once each option has been analysed, the strengths and weakness of the options are collected and summarised. Given that the objective is to select the lowest overall risk solution, each of the weaknesses are analysed further to identify their impact and subsequent risk posed to the project and to the final customer. Consideration is also given to the actions required to mitigate each of the risks.

Finally, a conclusion is reached that either recommends one option to proceed into Preliminary Design, or identifies further work to be implemented before a preferable solution can be selected. The conclusion is to be made based on overall risk, comparison of the practicability of mitigating actions for each weakness risk and assessment of the outstanding strengths of each option.

The conclusion also highlights any outstanding uncertainties/risks associated with the preferred option. These risks are recorded and then managed within the project's risk management process going forward.

5.2 Preliminary Design

GE has adopted a system engineering approach to the design and delivery of new tritium facilities. A system engineering approach was also adopted for the new Tritium Extraction Facility at Savannah River Site and the many advantages of this strategy are well documented [9].

By adopting a system engineering approach, requirements can be logically broken down for ease of requirement traceability. Identifying and defining systems also allows for categorisation of systems. This allows for the application of the most practicable level of rigor during the design and delivery of the project in concordance with the system's impact on overall stakeholder risk.

GE's Preliminary Design process is based upon methodology outlined in IEC61508 [10], however, the overall method has been extended to cover all safety, environmental and business mitigation measures.

The first stage of Preliminary Design moves the design from the Concept Design level block diagrams and technology choices to an early Design Intent. GE has defined Design Intent to mean overall system requirements, including intended modes of operation, location, boundaries, process conditions, inventories, emissions and system limitations.

This early Design Intent includes no safety, environmental or business risk reduction "add-on" measures (or extrinsic safety). Inherently low risk systems would already have been identified and incorporated into the design by following GE procedures, but specific "add-on" risk

reduction measures are excluded, (e.g. relief valves, containment and confinement systems, safety instrument systems, operator alarms & responses, etc).

This allows unmitigated risks to be identified and evaluated through a formalised Hazard Identification & Risk Analysis (HI&RA) review. This approach significantly helps the design process, and later the validation of the Design Intent, as each "add-on" measure can be validated against the criteria used during its selection.

Essential to GE's Preliminary Design process is this integrated involvement of safety and environmental hazard identification and risk analysis through the development of the design. This is in comparison to traditional safety reviews of a "final design", whereby engineers have somewhat arbitrarily selected safety measures and functions for the design based upon their own experience and personal what-if analysis, with little documentation of the objective and justification of the safety measures. This historical method of engineering and safety departments working in "silo" modes, with information passing back and forth in non-productive and non-collaborative fashion, leading to program delays, cost overruns and, more importantly, a loss of Design Intent as frequently the objective, reasoning and justification of the inclusion of the safety measures is lost.

The HI&RA used by GE is a systematic process identifying postulated hazards by a system of checklist and "what-if" analysis and then subsequent evaluation of the risk by deterministic means using a risk matrix.

A formalised GE Risk Reduction process is then used to apply mitigating solutions to reduce the risk to an ALARA or broadly acceptable level. The Risk Reduction process ensures that a traceable, controlled and consistent approach is adopted to the identification, evaluation and application of mitigating solutions, satisfying the Design Principles and subsequent Design Criteria. This approach is analogous to "System Modification" steps used to reduce the risks as described in the Framework for CPQRA Methodology [11].

This has many benefits for a customer; for example, during operation, if a relief valve needs to be removed from duty for maintenance, full traceability exists back to the original HI&RA and subsequent Risk Reduction evaluation meaning there is no ambiguity surrounding the Design Intent for the device.

Key to the success of this activity is GE's method to ensure that engineers conform to the Hierarchy of Risk Reductions Types (see Table 1). This is GE's interpretation of well-established and documented concepts embedded in most safety and environmental regulations and standards. The Risk Reduction process considers the relative costs of implementation overall effectiveness of different Risk Reduction solutions as illustrated by the following graphs:

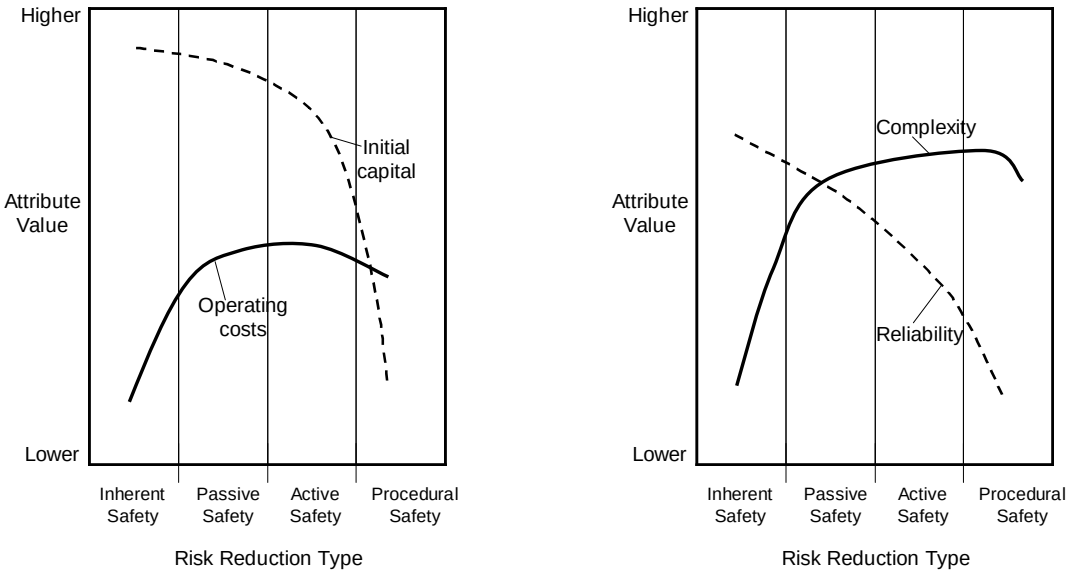

Figure 3: Comparison of typical cost and functional attribute by Risk Reduction Type (figure reproduced and modified based on illustration from reference 13)

Position in Hierarchy	Risk Reduction Type	Description & Examples
1	**Inherent**	Reduce the hazard inherently by reducing the quantity of hazardous material or energy or hazardous conditions, siting or by completely eliminating the hazardous agent or process
		Change of process to reduce hazardous inventory
	Passive	Do not require any device to sense and/or actively respond to a process variable and have very reliable mechanical design
2	Preventive	Increasing primary containment specification beyond fault conditions
3	Protective	Permanent guard around a hot surface
	Active	Require devices to monitor a process variable and a function to mitigate a hazard
4	Preventive	High level interlock preventing overfilling
5	Protective	Confinement system capturing spills
	Administrative	Require a person to perform an action to mitigate a hazard using operating procedures, administrative checks, emergency response, and other management approaches to reduce the probability or severity of the hazard
6	Preventive	High pressure warning event with operator response
7	Protective	Fire Alarm with emergency evacuation procedure

Table 1: GE's Hierarchy of Risk Reduction Types

GE's Risk Reduction process ensures that the design team can only consider moving down the hierarchy from a higher Risk Reduction type to a lower when it is not reasonably practicable to incorporate the higher reduction type. GE has used a custom designed database to help facilitate the process.

In GE's process of combining holistic hazard identification, risk analysis and then systematic risk reduction many of the various legislative requirements for hazard-related risk management, such as flammable atmospheres, overpressure, noise, ionising radiation, fire, external hazards,

environmental releases, etc. are all collectively addressed. Therefore, no separate reviews are required to individually address these topics (e.g. SIL determination, hazardous area zoning, etc) and there is consistency in the method by which these topics were addressed.

It has been proven that solely relying upon a risk-based approach for hazard management can have limitations [12]. Therefore, the GE delivery model incorporates a precautionary approach in the design process by the use of prescriptive standards to address significant top-down events. Such prescriptive standards include the use of containment and confinement systems when hazardous material inventory exceeds set thresholds, deployment of area monitors, minimum environmental abatement systems and electrical protection measures, etc, irrespective of whether the risk-based assessment identified the need for such safety measures. The use of a combined risk-based and precautionary approach ensures a robust safety case and demonstration of ALARA principles.

Given the nature of tritium, containment and confinement systems are often used to mitigate the consequence of release, followed by clean up where necessary. These systems also provide demonstrated methods to control the spread of radioactive contamination. The use of these systems adds to the complexity and cost of facilities and introduces significant ergonomic and access restrictions. Overly complex containment and confinement systems, like other safety measures, can reduce overall availability, increase the maintenance and inspection burden and, in some instances, introduce new hazards and fault pathways. The GE delivery model, however, provides procedures and guidance to ensure proper use and deployment of such systems. These procedures ensure that the Design Intent and safety functionality of the containment and confinement systems is logically and systematically selected and recorded. A formalised selection procedure is used to evaluate the grouping of such systems, thereby reducing overall cost in a controlled manner without the lost of functionality.

Once the Preliminary Design has incorporated the selected Risk Reductions, standard precautionary measures and required containment/confinement systems Hazard and Operability Studies (HAZOP) are conducted. GE's HAZOP procedure was developed following well established and published methodologies [13]. The HAZOP reviews are used to identify hazards that the design introduces and then identify risk mitigation solutions in place to prevent or protect against the hazard. Any new hazards introduced by the Risk Reduction 'add-ons' are also identified in the review.

GE's Hazard Analysis (HAZAN) process then systematically analyses the risks associated with the identified hazards. Any risks identified as not being ALARA or broadly acceptable following the HAZOP/HAZAN process are mitigated in accordance with the Risk Reduction process. The HAZAN includes both deterministic and probabilistic hazard analysis:

- The deterministic hazard analysis provides a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safeguards.
- The probabilistic hazard analysis is a structured and systematic assessment of the risks arising from a plant. It considers all potential fault sequences arising during the operations being considered by the safety report, derives frequencies for those fault

sequences, quantifies their consequences and from this provides an overall risk from the plant.

Finally after the analysis is completed categorization of the safety systems, structures and components is conducted. Categorization is determined according to their contribution to safety in order that they may be examined, inspected, maintained and tested with a level of rigour commensurate with their contribution to safety.

The Preliminary Design is concluded by incorporating the further Risk Reduction measures identified through the HAZOP/HAZAN process. These changes to the design are carried out in accordance with a formalised Change Control procedure to ensure that the HAZOP/HAZAN reflects the final design correctly.

Throughout the Preliminary Design phase, formalised and structured GE Design Reviews are conducted prior to the HI&RA, HAZOP and closeout review. The Design Reviews utilise extensive checklists and prompt words developed by GE and tailored to suit the particular system type under review. The checklists contain questions and prompts to ensure functional requirements of the systems are being met, full lifecycle considerations are addressed as well ensuring typical omissions and oversights are avoided based upon previous experience. The reviews are also used to ensure compliance to GE's engineering procedures and standards and incorporation of required Risk Reductions and precautionary measures after HI&RA.

5.3 Detail Design

GE's Detail Design phase concentrates on turning intent into reality via production of working drawings, specifications and tender/fabrication documents so that the facility and systems can be fabricated, assembled and tested.

During the generation of these deliverables, the Design Intent is maintained, or if a variation is unavoidable, the change to the Design Intent is properly managed through GE's Change Control procedure. Production, review, approval and management of these Detailed Design deliverables requires a methodical and comprehensive approach which GE achieves via an accredited ASME nuclear class and ISO9001 quality system.

Best practice is demonstrated by the use of GE Engineering Standards that have been specifically designed for tritium facilities. These standards and specifications cover all aspects, including primary containment, secondary confinement, building materials, process instrumentation & control, electrical components and HVAC. The use of these standards ensures compliance with relevant regulator requirements, inclusion of proven tritium compatible components and standardisation.

Standardisation helps to improve project delivery via reducing time-inefficient custom component searching and increases procurement leveraging by concentrating component sourcing. Significant advantages for the end-user are also realised by providing a platform for common training in component identification and use while reducing onsite spares holding.

6. Design Substantiation

Substantiation of the design aims to show that the Design Intent is capable of meeting all requirements of the customer, legislation and best practice.

GE has adopted a progressive design substantiation process for delivery of tritium facilities. In this approach, substantiation to the URS and Design Principles is conducted as the design progresses. This is in comparison to the traditional method of waiting for a final design to be created and then conducting a review by independent groups to verify the design.

The advantage of the progressive approach is that frequent review activities by independent groups can help steer and direct the team to success, reducing rework and cost overruns. Bringing the independent review team along with the development of the project also brings the advantage that they are better informed and fully understand the Design Intent.

Given the lack of prescriptive requirements for tritium facilities, traditional substantiation processes have had the tendency to be very subjective and time consuming. The GE design substantiation process overcomes this by ensuring substantiation to the Design Principles in particular is demonstrated by reviewing how the Design Intent has been developed.

The substantiation process is further improved by GE's adoption of a central requirements management database [14]. The advantages of using such as system include:

- Supports multiple users working simultaneously allowing every user, at any given moment, full access to the most recent versions of all requirements
- Ability to automatically trace the impact of any requirement change
- Ability to quickly navigate links between requirements during reviews
- Ability to show traceability between all levels of requirements, allowing users to automatically identify any high-level requirements that have not yet been addressed

Overall the GE method used represents best practice for requirement traceability and has received very positive feedback from regulators and customers.

7. Conclusion

GE's design and delivery process for new tritium facilities has four important aspects:

1. Establishment of jointly agreed URS and Design Principles that are used to select the most appropriate options for technology, location and facility design via structured comparative risk-based option studies to create the Concept Design for the new facility.
2. Preliminary Design that divides and categorizes the facility into systems that have their Design Intent systematically defined by first assessing unmitigated safety, environmental and business risks throughout the lifecycle of the facility, each risk is subsequently

reduced to ALARA following a safety hierarchy and then detailed hazard analysis follows which confirms overall facility safety.

3. Best practice is continued into Detail Design by the use of internationally recognized nuclear accredited quality systems, compliance with GE Engineering Standards that have been specifically designed for tritium facilities and, finally, standardization of components which improves project delivery and reduces training and spares holding.
4. Throughout all design activities and into fabrication, assembly, testing, commissioning and facility handover into operation, a progressive substantiation process of requirements traceability is systematically controlled and executed through the use of a computer application that allows transparent demonstration of compliance.

With the likelihood that more tritium facilities will be required in the future as CANDU® new build begins, projects that deliver these facilities would significantly benefit from adopting these approaches.

8. References

1 "Handbook: Tritium Handling and Safe Storage", US Department of Energy, DOE-HNDBK-1129-99 (March 1999)
2 "Radioactive Waste Recovery and Enrichment", Bonnett I., Busigin A., Lashford A., Williams H.R.P., 9th International Symposium on the Synthesis and Application of Isotopes and Isotopically Labelled Compounds, Edinburgh, July 16-20, 2006
3 "A Guide to the Project Management Body of Knowledge"ANSI/PMI 99-001-2004, Project Management Institute, 2004
4 "Safety Assessment Principles for Nuclear Facilities", HSE, 2006
5 'Safety of Nuclear Power Plants: Safety Design Requirements", International Atomic Energy Agency (IAEA) Safety Standard NS-R-1, 2000
6 'Area Classification Code for Installations Handling Flammable Fluids IP Part 15', Energy Institute, 2005
7 'Inherent Safer Chemical Processes – A life Cycle Approach', CCPS, AIChE, 1998
8 'Guidelines for Engineering Design for Process Safety', CCPS, AIChE, 1993
9 "Application of the Systems Engineering Approach to the Tritium Extraction Facility Design", P Simpkins, Rpt No. WSRC-MS-2002-00822, Westinghouse Savannah River Company
10 "Functional Safety of Electrical /Electronic/ Programmable Electronic Safety Related Systems", International Electrotechnical Commission, Standard IEC161508, 2000
11 'Guidelines for Chemical Process Quantitative Risk Analysis', CCPS, AIChE, 2000
12 "Management of chemical exposure: the limitations of a risk-based approach", Santillo D., Johnston P., Stringer R., Int. J Risk Assessment and Management 2000 - Vol. 1, No.1/2 pp. 160-180
13 'Guidelines for Design Solutions for Process Equipment Failures', CCPS, AIChE, 1997
14 "From Document To Database:Modernizing Requirements Management", Giajnorio J. & Hamilton S, 28th Annual CNS Conference & 31st CNS/CNA Student Conference, Saint John, New Brunswick, Canada, June 3 – 6 2007