A REVIEW OF SAFETY BY DESIGN CONCEPT IN ELECTRIC UTILITIES

Muhammad Arshad, Syed M. Islam and Abdul Khaliq

Abstract **There is a remarkable correlation between quality management and safety through design philosophy. In general, a more reliable plant is a safer plant. Equipment in modes of operation not anticipated by the designer can create significant risks. There is a large difference between the predicted performance of systems and those observed in practice including the management of deviations, constraints of production, extending the life of equipment, evolution of production systems, process variability, etc. This gap is considered currently as one of the main causes not only of poor performance, but also of risk taking by operators, because they have to respond to situations which have not been considered in the design phase. Business objectives of survival, return on investment, cost control and reduction, and their effect on operating managers serve as reminders that good data must be accumulated to support the social and moral considerations in promoting changes to reduce hazards to an acceptable level. This paper presents the concepts of cradle to grave aspect of safety through design, change in safety philosophy, safety management structure and specific initiatives such as training, communications, incident analysis, safety audit, new procedures, tools, equipment and work methods.**

I. Introduction

The new objective-based safety standards ensure that the requirements continue to accommodate design innovations, build on established industry experience and practice, and promote cost-effective and flexible solutions to maintain the high levels of safety the public and the industry have come to expect. A safety analysis during the design phase identifies unnecessary hazards. Safety integration in design encourages harmonizing and supplementing the regulatory requirements resulting in enhanced safety of personnel, equipment and facility. Safety by Design consideration minimizes electrical utilities operational and maintenance risks [1].

The introduction of new technologies has increased the performance of the systems in terms of quality, productivity, flexibility and availability. However it is very difficult for the designer to take account of all the relevant factors relating to health, safety and the integration of operator activities/interventions. Emerging electrical safety concerns are complicated to be addressed as they involve both scientific and cultural changes. Integrating safety in the design stage to improve safety will inflict high cost on the facilities [2-3].

Review of basic purpose and concepts of the project is required, emphasizing and offering insights into a wide variety of costs and their importance in relationship to the acceptance and implementation of safety through design concepts. Introduction of the concepts of life cycle costing and recycling costs as important tools in this whole process emphasizes the cradle to grave aspect of safety through design. Safety by Design decision for planned and unplanned maintenance would affect equipment/system maintainability and serviceability and minimize the failure probability. It is difficult to predict the future safety risk by measuring accident severity rate and lost time injury frequency rate. Also due to the aging of power equipment the performance and conditions of these assets may deteriorate and that may escalate safety risks [4].

Literature on maintenance, operation, and reliability rarely addresses designing for minimum risk of injury for the related workers. Also many organizations design for planned maintenance, but unplanned maintenance will account for the vast majority of downtime. Safety through design requires that these tasks be defined. The system design failure modes often forces the safety professionals to find undocumented details of the system behaviour [5].

Once the concept of avoiding error-provocative work situations is accepted, engineers and safety practitioners are in a good position to review existing situations with a different perspective. The importance of recognizing circumstances where retrofitting can come into play is stressed. There will be numerous instances where retrofitting of existing equipment and processes will be necessary and safety through design principles can be applied. In identifying situations requiring retrofitting, the role of safe job procedures and accident/incident investigation in the process are required to be reviewed. Modifications of existing products, equipment, and processes provide an excellent opportunity to conduct a risk assessment of the original design and to evaluate it against the current state of technology. An organization may be expending excessive resources on equipment which is not really critical. At the same time, the department might not be devoting enough attention to the equipment that is really critical, reducing the reliability, safety, and profitability of the plant.

In general, a more reliable plant is a safer plant. Equipment in modes of operation not anticipated by the designer can create significant risks, the highest risk phases of operation are start-up and shutdown. Designer should

Manuscript received October 23, 2007.

M. Arshad is with the BC Hydro, Generation Engineering Maintenance Services, Canada (muhammad.arshad@bchydro.bc.ca)

S. Islam, Department of Electrical Engineering and Computer Engineering, Curtin University of Technology, Perth (S.Islam@curtin.edu.au).

A. Khaliq is with the Department of Electrical and Computer Engineering, Islamabad, Pakistan.

consider required maintenance during design, ensuring that maintenance operations can be safely performed while the plant operation continues. Safety integration in the design requires highly interactive reviews by the design engineers, end users and safety professionals [6].

The frequency of accidents, which occur represent the difficulty to ensure the systems to operate safely. Due to the recent rapid development in the technology, accidental design faults might cause safety concerns to the human life and environment. For safety assurance critical systems/components are required to have a verification process [7]. The European Union (EU) introduced a new approach to technical harmonization and Standards aimed at integrating safety at the design stage [8]. The EU Machinery Safety Directive sets out Essential Health and Safety Requirements (EHSR) for machinery which must be met before machinery is placed on the market anywhere within the EU. EHSR s are expressed in general terms and it is intended that the European Harmonized Standards should fill in the detail so that machinery designers and suppliers have clear guidance on how to achieve compliance with the Directive and to integrate safety at the design stage. The EU Directives represent a remarkable breakthrough in risk-based approach to equipment and work safety. Research and investigations show that the majority of machinery suppliers into the UK market have failed to demonstrate compliance with the risk based approach.

II. Safety Management

To plan, design and implement a safety management system that neither workplace conditions, nor the action of the people exposes personnel unnecessary to hazards. The main objective is to describe a methodology for determining safety integrity level requirements for the overall safety, this includes:

1) Propose definitions of equipments under control for local and global safety functions.
2) Describe the required extent of hazards and risk analysis.
3) Describe minimum safety integrity level requirement and how to identify deviations from these requirements.
4) Propose suitable methods for handling deviations from the minimum safety integrity level.

The safety management basic challenges are to:

1) Protect people, property and environment.
2) Manage risk.
3) Limit liability.
4) Meet government and industry regulations and guidelines.

III. Safety by Design

Integration of safety and human factors into the design phase is therefore essential if the expected performance is translated into achieved results in a system. It is becoming increasingly common to require a safety case be provided for a safety-critical system prior to its deployment [9]. One of the key aspects of design is that in case of failure it should fail in a benign mode. The designers are faced with several problems during the design phase, these include the following [8]:

1) The lack of sufficient site specific data relating to new design.
2) The lack of ability to foresee variable human interventions, and the respective associated hazard.
3) Identification of probable misuse of machine in particular while dealing with operation and maintenance procedures.
4) Hazard and risk assessment experts support to assist the designer in integrating health and safety into the design.
5) Bringing together a number of different types of expertise.
6) Design conflicts between various engineering disciplines professionals/designers.
7) The functional analysis and assessment e.g. operator intervention on the system.

A. Risk Assessment

This involves the probability of exposure to the harm inside the danger zone coupled with the consequences of exposure. It also considers evaluation of risk and whether corrective/preventive measure is needed to reduce risk to a tolerable level. The risk assessment is essentially a proactive approach based on a structured and systematic method for hazard identification, evaluation of risks and decision to reduce risks to a tolerable level [8]. The risk of unexpected failures ranges from minimal to very high depending upon the concern utility s level of redundancy. The losses include damage to equipment, system operations, safety and the environment. The risk management would reduce the overall risk exposure in terms of costs, service reliability and availability. Asset s assessment is vital to determine its technical end of life, practicable performance, strategic and economic impacts. To develop advanced life cycle management strategies for the asset, the following criteria provides basis to maintain its good operational reliability and availability.

1) Identification and impact of major risks that may be present in the transformer.
2) Identification and impact of existing risks on the system and environment.
3) Implementation of cost effective procedures to reduce the failure risk.
4) Alternate action in the absence of failure prevention.

It is important to understand the four main phases of protection from electrical hazards [10].

1) Electrical installations should be designed and constructed to be safe by complying with the criteria of

recognized and generally accepted good engineering practices.
2) The integrity of electrical equipment shall be maintained with particular emphasis on enclosures, insulation, operating mechanisms, grounding, and circuit protective devices.
3) Unless there are serious overriding circumstances, electrical equipment shall be placed in an electrically safe work condition before personnel work on or near it. Safe practices shall be used to establish an electrically safe work condition.
4) Safe work practices and adequate protective equipment, tools, and test equipment shall be understood and used when it is not feasible to establish an electrically safe work condition, or when de-energizing would create a greater hazard of another kind.

The two basic risk assessment techniques, which are considered more relevant to machinery safety, are the hazard-based approach and the task-based approach. The task-based risk assessment is much more open-ended as it analyses different hazards associated with each step of the task/subtask. There is an ample safety and environmental risk involved in operating aged assets. Asset s risk assessment and mitigation strategies mainly depend on the preventive, corrective and reliability centred maintenance programs associated with condition monitoring. Condition monitoring is mostly considered for transformer insulation system and winding integrity and would focus on the following identifications of the asset [11]:

1) Highest failure rate.
2) Strategic importance.
3) High concern irrespective of failure rate.
4) Serving close or beyond its design life.

For accurate risk assessment a comprehensive knowledge of the following parameters is required.

1) Component and material used in the construction of equipment/system.
2) Factors controlling/influencing the deterioration and failure of the asset.
3) Asset function with respect to performance standards.
4) Types of failure.
5) Sources of failure.
6) Failure rate.
7) Deterioration rate.
8) Manufacturer test data.
9) Failure historical data.
10) Failure analysis.
11) Failure effect on the system (outage down time, reliability, safety, revenue loss, environmental damages and repair/ replacement cost).

To integrate safety in the design, in-depth knowledge of the asset s design, operation, stresses, monitoring, diagnostics and maintenance is required. The risk assessment is mainly based on the performance and failures historical data. Causes of failures and respective consequences investigation stand vital for the asset management point of view. Failure probability analysis is also a key parameter in asset management. Risk assessment is a key instrument in the asset management. It facilitates failure analysis to predict the causes and their impact on the over all system. Also diagnostics and monitoring techniques provide useful information for developing and implementing safety by design strategies.

1) Example Transformer Risk Assessment:

Transformers are an integral part in ascertaining the reliability of any power utility. The operational availability of large power transformers is of strategic importance for power generation and transmission companies. There is an ample safety and environmental risk involved in operating aged units close to loading limits with out surveillance and assessment. Serious failures in power transformers owing to insulation breakdown cause considerable financial losses due to power outage and costs for replacement or repair. Therefore, most power utilities have developed individual inspection methods and schemes for the transformer condition assessment and they traditionally collect duty time percentage data and information on failure causes. Due to the majority of the transformers reaching significant age, there exists an interest of failure rate reduction.

A recent survey estimates that power outages cost each of the roughly two million US industrial and digital economy electricity customers more than $23,000 per year. Utilities are interested in safely maximizing the use of assets, minimizing interruptions to customers, and enhancing shareholder s value. It is essential to achieve goals such as optimization of the maintenance, loading, and life of the key transformers in our system. Transformer failure survey statistics shows that; electrical disturbances (29%), deterioration of insulation (18%), lightning (16%), inadequate maintenance (13%), loose connections (13%), moisture (7%), and overloading (2%) are the main causes of failure [12].

According to an IEEE transformers survey, oil immersed transformer failure rate per unit year is 0.00625. Therefore in a fleet of 100 transformers, ten will have problem with in next 16 years. An international survey of CIGRE, shows typical failure rates for large power transformers for operating voltages up to 300 kV is in the range of 1% to 2% p.a [13]. The failure rate is three times higher in utilities with poor maintenance programs then others, having better maintenance programs [14]. It is expensive to replace the existing aging transformer fleet as some may still in good working condition [15]. Power Transformer risk assessment and management challenges are due to the following reasons [16-18]:

1) Many transformers are expected to operate at or above nameplate ratings.
2) Peak loads are exceeding design limits resulting in smaller safety margins.
3) Equipment replacement lead times can be greater than one year.
4) Transformer average age continues to increase.

5) Transformer operating beyond its rating experiences the followings:
   - Increase in temperature of windings and insulation, causing insulation deterioration.
   - Increase in leakage flux density outside the core, causing additional eddy current heating in the metallic parts linked with flux.
   - Increase in the moisture and gas content.
   - Bushings, tap-changers, current transformers and cable end connections are exposed to a higher stresses.
6) Spot market replacement power costs are unpredictable and will likely continue to rise.

To apply safety by design criteria for the aging asset it is highly recommended implementing online monitoring devices and diagnostic tools to have continuous and accurate assessment.

Another example of safely by design is replacing fuse with circuit breaker for fault clearance. A typical Arc Flash incident Energy is 50Cal/cm^2 for a 13.8kV/480V circuit having fuse to clear the fault (typically 08.S); whereas replacing the fuse with rely/breaker arrangement for the same circuit would reduce the Arc Flash energy to 15Cal/cm^2 (typically clearing time is 0.4S).

B. Safety Criteria in the Design Stage

Safety is considered as a main concern in engineering design. The international standard IEC 61508 has been generally accepted as the foundation for specification, design and operation of Safety Instrumented Systems. The standard sets out a risk-based approach for deciding the Safety Integrity Level for systems performing safety functions. The design of safety-instrumented systems using a risk-based approach and realization of safety systems is a highly specialized expertise. Risk based design of safety instrumented systems aims to establish the risk reduction that to arrive at an acceptable tolerable remaining risks [19]. A safety instrumented design system would require the following inputs:

1) Equipment/system definition.
2) Site specific requirements.
3) System integrity and performance criteria.
4) Codes, safety, performance, design standards and specifications.
5) Faults and hazard identification and risk assessment, identification of various major safety risk probabilities and impacts that may be present.
6) Mitigation procedures and strategies against abnormalities.
7) Risk consequences and emergency procedures.
8) Operation and maintenance safety protocols.
9) End-of-life and decommissioning strategies.
10) Probabilistic safety analysis.
11) Criteria for choosing the design basis faults.
12) Validation process to verify that the plant will deliver safely.

IV. RECOMMENDATIONS

It is recommended that functional safety assessments be made at the following stages:

1) After the hazard and risk assessment has been carried out, the required protection layers have been identified and the safety requirement specification has been developed.
2) After the safety system has been designed.
3) After the installation, pre-commissioning and final validation of the safety instrumented system has been completed and operation and maintenance procedures have been developed.
4) After gaining experience in operation and maintenance.
5) After modification and prior to decommissioning of a safety instrumented system.

V. CONCLUSIONS

A safety analysis during the design phase will identify unnecessary hazards, many of which may be designed out through the use of alternative components, systems, or construction methods. The safety by design consideration would allow an aappropriate action in new and developing safety issues, industrial hygiene, ergonomics, loss prevention and environmental control. This will also provide enhanced safety management program with new safety concepts and techniques.

REFERENCES

[1] Mohla, D.; McClung, L.B.; Rafferty, N.R., "Electrical safety by design," *46th Annual*, *Petroleum and Chemical Industry Conference, 1999. Industry Applications Society* vol., no., pp.363-369, 1999.

[2] McClung, L.B., "Benchmarking safety," *IEEE Industry Applications Magazine,* vol.9, no.3, pp. 10-15, May-June 2003.

[3] McClung, L.B., "Results of formal benchmarking electrical safety," *48th Annua*l, *Petroleum and Chemical Industry Conference, 2001. IEEE Industry Applications Society* vol., no., pp.337-344, 2001.

[4] Hamoud, G.; Toneguzzo, J.; Yung, C.; Wong, A., "Assessment of asset safety risk for transmission stations," *IEEE Power Engineering Society General Meeting, 2006.* vol., no., pp. 7 pp.-, 18-22 June 2006.

[5] Joshi, A.; Miller, S.P.; Whalen, M.; Heimdahl, M.P.E., "A proposal for model-based safety analysis," *The 24th Digital Avionics Systems Conference, 2005. DASC 2005.* vol.2, no., pp. 13 pp. Vol. 2-, 30 Oct.-3 Nov. 2005.

[6] Hulet, M.W., "Advanced management of safety," *Proceeding, Annual Reliability and Maintainability Symposium, 1994.* vol., no., pp.37-39, 24-27Jan 1994.

[7] Hsiung, Pao-Ann; Chen, Yean-Ru; Lin, Yen-Hung, "Model Checking Safety-Critical Systems Using Safecharts," *Transactions on Computer*, vol.56, no.5, pp.692-705, May 2007.

[8] Raafat, H.; Simpson, P.; Integrating safety during the machine design stage , *International Safety in Design Congress 2000,* 13-20 October 2000, Orlando, Florida.

[9] McDermid, J.A., "Proving the design in the safety case," *IEE Colloquium on Designing Safety-Critical Systems,* vol., no., pp. 7/1-7/4, 1994.

[10] IEEE Std. 902-1998, IEEE Guide for Maintenance, Operation, and Safety of Industrial and Commercial Power Systems.

[11] D. Allan, "Condition Monitoring and Life Assessment of Aged Transmission/Sub Transmission Plant (Part A & B)," Powerlink Queensland, Australia 1997.

[12] Augenstein, W. Fox, and P. Fischer, "Outsourced monitoring and reliability of critical assets," in *Distributech*: Serveron Corporation, Feb. 4-6, 2003.
[13] "An International Survey on Failures in Large Power Transformers," CIGRE WG 12-05 1983.
[14] M. Belanger, "A Statistical Justification for Preventive Maintenance," Transformer diagnostics- Part 1.
[15] T. K. Saha and P. Purkait, "Investigation of polarization and depolarization current measurements for the assessment of oil-paper insulation of aged transformers," *Dielectrics and Electrical Insulation, IEEE Transactions*, vol. 11, pp. 144-154, 2004.
[16] D. J. Vanier, "Asset Management 101, A Primer," presented at APWA International Public Works Congress NRCC/CPWA Seminar Series Innovations in Urban Infrastructure , Canada, 2000.
[17] V. Sokolov, "Transformer Life Management," presented at II Workshop on Power Transformers-Deregulation and Transformer Technical, Economic and Strategical Issues, Salvador, Brazil, 29-31 August 2001.
[18] W. H. Bartley, "Life Cycle Management of Utility Transformer Assets," presented at Breakthrough Asset Management for the Restructured Power Industry forum, Salt Lake City, UT, October, 2002.
[19] Wiegerinck, J.A.M., "Introduction to the risk based design of safety instrumented systems for the process industry," *7th International Conference on Control, Automation, Robotics and Vision, 2002. ICARCV 2002.* vol.3, no., pp. 1383-1391 vol.3, 2-5 Dec. 2002.