CHEMICAL ENGINEERING TRANSACTIONS

VOL. 26, 2012

A publication of

AIDIC

The Italian Association
of Chemical Engineering
Online at: www.aidic.it/cet

Guest Editors: Valerio Cozzani, Eddy De Rademaeker
Copyright © 2012, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-17-4; **ISSN** 1974-9791

DOI: 10.3303/CET1226046

Human Factors Issues and the Risk of High Voltage Equipment: Are Standards Sufficient to Ensure Safety by Design?

Maria Chiara Leva*[a], Roberta Pirani[b], Micaela De Michela[b], Paul Clancy[c]

[a]APRG School of Psychology Trinity College Dublin, Ireland
[b]Dipartimento di Chimica Politecnico di Torino, Italy
[c]Asset Management ESBI Dublin Ireland
levac@tcd.ie

High voltage equipment is mostly designed according to technically prescriptive standards requirements based on electrical engineering safety principles. However a more risk-based approach to standards and regulation may be advisable to enable designer and user to take an active role in establishing that their installation is inherently safe. The use of Gas Insulated Switchgear (GIS) for instance is enabling the new substation to be housed indoors and condensed into around one quarter of the space. The manufacturers argue that design improvements in GIS make it virtually “maintenance free”, comply with all the relevant standards. However some of these improvements have implications for the operators that need to be taken into account. Commissioning, operational checks and inspections and the occasional maintenance interventions are activities during which the technicians need to interface with the equipment, the issues regarding the interfaces provided have been analysed to identify their relevance in the overall risk assessment of the equipment. The paper reports about a study aimed at verifying through a risk analysis the impacts that the issues related to deficit in ergonomic design may present for the overall availability and safety of the plant. Those issues are not tackled in the technical standards and/or designers current practice.

1. Background of the study

Several research projects and programs on system safety engineering and Quantitative Risk Analysis in the last 40 years offered very strong evidence of the crucial role that human and organizational factors (HOFs) play in major accidents. According to this increasing concern toward the relevance of HOFs in limiting safety performance considerable research effort has been spent worldwide in the last couple of decades. This resulted in quite a rich literature covering areas from theoretical bases, to accident investigation methods and application to major disasters, to very sophisticated modelling approaches and techniques of HOFs in Quantitative Risk Analysis and many standards trying to incorporate more physical aspects of Human factors like Ergonomics design. Nevertheless, many of the models and applications described in scientific literature demonstrate very limited impact on the technical standards applied for evaluation of safety critical equipment and procedures. The standards used for providing requirements of High voltage equipment for instance do not take into proper account aspects related to the human limited but by no means negligible interaction with the equipment. High voltage equipment is mostly designed according to technically prescriptive standards requirements based on electrical engineering safety principles (CEI IEC 62271-202, 2006). However a more risk-based approach to standards and regulation may be advisable to enable designer and user to take an active role in establishing that their installation is inherently safe. The use of Gas Insulated Switchgear

Please cite this article as: Leva M.C., Pirani R., Demichela M. and Clancy P., 2012, Human factors issues and the risk of high voltage equipment: are standards sufficient to ensure safety by design?, Chemical Engineering Transactions, 26, 273-278
DOI: 10.3303/CET1226046

(GIS) for instance is enabling the new substation to be housed indoors and condensed into around one quarter of the space. The manufacturers argue that design improvements in GIS make it virtually "maintenance free". However some of these improvements have implications for the operators that need to be taken into account. A GIS more compact in fact often means having awkward stations for the technicians during commissioning and maintenance actions that are still required to be performed. Commissioning, operational checks and inspections and the occasional maintenance interventions are activities during which the technicians need to interface with the equipment, the issues regarding the interfaces provided have been analysed to identify their relevance in the overall risk assessment of the equipment. The scope of the present study is to verify trough a risk analysis the impacts that the issues related to deficit in ergonomic design may present for the overall availability and safety of the plant. Issues overlooked by both the technical standards and the designers.

2. The need for risk informed design in GIS

The term switchgear, used in association with the electric power system, or grid, refers to the combination of electrical disconnects, fuses and/or circuit breakers used to isolate electrical equipment. Switchgear is used both to de-energize equipment to allow work to be done and to clear faults downstream. This type of equipment is important because it is directly linked to the reliability of the electricity supply. A safe, reliable supply of electricity depends on the circuit breakers that protect our electricity grids in the event of short circuits. An effective although more costly form of switchgear is gas insulated switchgear (GIS), where the conductors and contacts are insulated by pressurized sulphur hexafluoride gas (SF6). The use of GIS rather than conventional air insulated switchgear (AIS) is enabling the new substation to be housed indoors and condensed into around one quarter of the space. Gas Insulated Switchgear have been gradually changed, moving towards layout that require less and less space and often means having less space and awkward stations for the technicians during commissioning and maintenance actions.
Figure 1 shows an overall vision of the most important components of the GIS that are involved in the commissioning and maintenance phase. Figure 1 represents a section of the GIS system (not to scale).

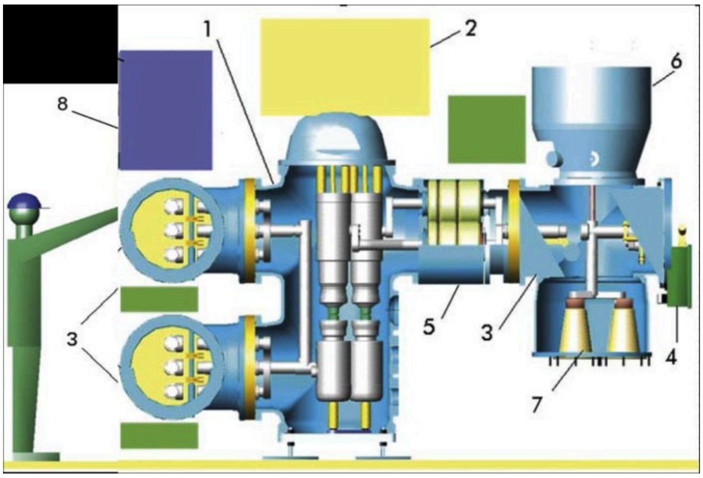

Figure.1 Cross Section View of GIS

The designers and manufacturers often refer to GIS as maintenance free, however commissioning, operational checks and inspections and the occasional maintenance interventions are activities during which the technicians need to interface with the equipment and the issues regarding the interfaces provided have been analysed to identify their relevance in the overall GIS risk assessment.
The study highlights clearly that good design, taking into account all potential risks, helps to ensure safety during repair and maintenance work. It demonstrates once again the importance of taking into account human factors at the design stage of a piece of equipment; where modifications are easier to

carry out and less expensive than they would be once the plant is built. The end users of the machine were actively involved throughout the whole risk assessment process and played a crucial role in ensuring an evaluation of the conditions leading to a safe commissioning and operations of GIS.

This study was also used to evaluate whether current standards used for the design and operation of High voltage equipment (CEI IEC 62271-202, 2006) are sufficiently taking into account the relevant aspects of man-machine interface.

To achieve the objective, a preliminary risk assessment has been performed on an installation complying with relevant standards (IEC 62271-202, 2006; IEC 62271-1, 2007; IEC 62271-203, 2004).

3. The use of an extended FMEA for taking into account Human Operations

The Risk Assessment was performed using an ad hoc Failure Mode and Effects Analysis (FMEA) template where the functional analysis included the human tasks as well as the technical aspects.

The risk levels associated to each possible failure mode were obtained using the risk matrix proposed by a US Military standard used for FMEA analysis (MIL-STD-882, 1993). The overall method aimed at providing the assessment of a Risk Level similar to the Safety Integrity Level evaluation required by standards (EN IEC 61508, 2002) (originally developed for process plants, machineries and vehicles contain requirements and recommendations for validating safety-related electrical, electronic and programmable control systems).

The method would start with a functional analysis of the equipment to identify all the relevant functions to be performed by the equipment or by an operator and the connected failure modes. Some of the failure modes can be determined assessing the Human Errors using the Technique for Human Error Rate Prediction (THERP) developed for the U.S Nuclear Regulatory Commission (Swain and Guttman, 1983). Information about the order of magnitude of the likelihoods of the events was obtained using equipment reliability data (when available) and THERP for relevant human errors. The severity of the outcomes was assigned using expert judgment based on the classifications guidelines proposed in the US military standard that provides guidelines for FMEA analysis (MIL-STD-882, 1993).

The template used identifies the man-machine functions as a starting point for the functional analysis column. The phases of the analysis performed are:

1. Functional analysis for man and machine actions at different stages of the plant lifecycle (the only one considered are commissioning, normal life, maintenance. Decommissioning and installation were not considered for the purpose of the analysis)
2. Identification of the key tasks
3. Identification the failure modes for the components and error modes for the operator tasks involved in the operation
4. Detection of causes and consequences of the human error or failure of the device involved in the task

Table.1: Hazard severity (category are compared with the one proposed by a standard used for safety of machinery (IEC 62061 2005)

Category	Name	Characteristic
I (4)*	Catastrophic	Death / Loss of system
II (3)	Critical	Severe injury or morbidity/ Major damage to system
III (2)	Marginal	Minor injury or morbidity/ Minor damage to system
IV (1)	Negligible	No injury or morbidity (first aid)/ No damage to system

Once the qualitative analysis was completed the next step was the evaluation of the appropriate reliability data to be used for the quantitative assessment. For the quantification of the hazards in terms of severity of consequences and likelihood of occurrence, we have adopted the same approach proposed in the standard commonly used for safety of machinery (IEC 62061, 2005) with the purpose to follow the guideline used in the field of safety of machinery for the establishment of a Safety Integrity Level. To apply the hazard assessment matrix (Table 3) to evaluate whether the risk was unacceptable or acceptable it was necessary to translate the numerical values, obtained from the quantitative analysis, in a judgment (Tables 1 and 2). The choice of range in which likelihood and severity of consequences fall, are in line with the guidelines proposed by a US Military standard (MIL-STD-882 1993).

Table.2: Categories of Hazard likelihood where the category given by the Military standard is aligned with the one proposed by a standard used for safety of machinery (IEC 62061 2005)

Category	**Name**	**Characteristic**	**Probability ref. [event/y]**
A (5)*	Frequent	Likely to occur frequently/ Occurred several times in the last 5 years in the company.	$> 10^{-1}$
B (4)	Probable	Will occur several times in life of a component. Has occurred in the company.	10^{-1} to 10^{-3}
C (3)	Occasional	Likely to occur sometimes in life of a component. Has occurred more than once in the industry.	$< 10^{-3}$
D (2)	Remote	Unlikely but possible to occur in life of a component. Has occurred in the industry. No damage to system	$< 10^{-4}$
E (1)	Improbable	Occurrence may not be experienced. Never occurred in the industry	$< 10^{-6}$

Table.3: Tools to define the class of risk: Hazard Assessment Matrix and Hazard Risk Index

Frequency of occurrence	**Hazard severity**			
	I Catastrophic	**II Critical**	**III Marginal**	**IV Negligible**
A - Frequent	**RI 1**	**RI 1**	**RI 1**	**RI 3**
B - Probable	**RI 1**	**RI 1**	**RI 2**	**RI 3**
C - Occasional	**RI 1**	**RI 2**	**RI 2**	**RI 4**
D - Remote	**RI 2**	**RI 2**	**RI 3**	**RI 4**
E - Improbable	**RI 3**	**RI 3**	**RI 3**	**RI 4**

The quantitative analysis required to identify the likelihood and consequences related to a variety of events like failure mode of the electrical components, human error, “falls from ladders”, etc. and for this reason these values have been obtained from different sources.

Failure rate of electrical device were provided by reliability data of the manufacturer or through GESCOM data base (CESI, 2005) related to reliability of the components of the Italian electricity grid. In this last case the value was not related to each single component but it refers to the whole system; from the MTTF (Mean Time To Failure) it was possible to obtain the respective failure rate using the following relation: $MTTF = 1/\lambda$.

Likelihood of events like “falls from ladders” derives from expert judgment and from records of worker’s injury reported by the company involved in the analysis.

3.1 The contribution of possible human errors and their influencing factors

The failure rate values associated to human error were obtained through the application of THERP model (Swain and Gutman, 1983). THERP (Technique for Human error Rate Prediction) is a method to predict human error probabilities and to evaluate the degradation of a man-machine system likely to be caused by human errors alone or in connection with equipment functioning, operational procedures and practices, etc.

THERP requires the analyst to determine whether the error to be examined is one of omission, one of commission, or diagnosis and sources of operator burden include the following: a) time constraints, b) diagnosis, c) physiological factors, etc. The data for human error probability (HEP) in THERP tables referred to the assumption of a lognormal distribution for the human error probability density function (truncated in 0 and 1). In the tables two values are reported: the median of the distribution and error factor. From this two values the mean value for the lognormal distribution is obtained to be used for assessing the final HEP. For those ergonomic constraints that could actually prevent the job from being effectively carried out it was assigned factor 10, for those constraints that could force the operator to err a multiplication of a factor 5 was used. The likelihood obtained was also discounted to take into account the actual timeframe over which certain tasks are carried out in the life period of the equipment (e.g. commissioning is 1/ 30 years, where 30 years is the expected life duration of the equipment, and Maintenance interventions 1/ 5 years)

4. Main findings of the assessment

The study shows that the most significant issues are:

- often limited and restrictive working areas;
- the technician has to work in fixed and awkward posture for sustained periods of time,
- difficulty or complete inability of reading the metrological data,
- slowdown in emergency procedure.

Most of these issues are ergonomic aspects and they have an important relapse on reliability of the whole system and on the wellbeing of the operators. It seems that some basic principles of accessibility were not properly taken into account in the design of the equipment. The lack of basic ergonomics principle in design is reflected in the difficulties encountered by the operators to manually open or close the circuit breakers in case of failure of automatic activation. The risk is that the worker may fail to resolve possible critical situations in time because he/she must reach the high location and turn the mechanism shaft while standing in an awkward position.

The results of the first step of the analysis are confirmed and supported by a survey of users of GIS carried out by the Committee of the Institute of Electrical and Electronics Engineers (IEEE, 2010).

The results provided by the quantitative analysis suggest two types of consequences. The first is related to the underestimation of the risk associated with the loss of primary functions of the plant normally achieved with a traditional FMEA, the failures connected to loss of efficiency, possible disruption to customers seems to be much higher and diverse than the one normally considered in common FMEA performed on that type of equipment (Buakaew, 2010). Once applied the hazard assessment matrix the hazard risk index for each failure mode falls into two different classes: Risk index 1 and Risk index 2. One is unacceptable (Risk index 1) the other risk index commonly obtained (Risk Index 2) refers to undesirable situations where the operation is possible but awkward to perform such that the operator may be more easily induced to make mistakes. In those cases the consequences are severe both for the operator safety and for the plant efficiency.

Table 5 contains an extract of the results obtained for the risk Assessment of the GIS with some examples of the failure modes leading to a risk index 1 or 2.

5. Conclusions

The analysis results confirm that the accessibility of the GIS presents different crucial aspect that the basic standards for High voltage equipment (IEC 62271-1, 2007; IEC 62271-203, 2004)and the manufacturer did not take into proper account.

The technical regulation IEC related to GIS is not completely exhaustive for the aspects of detail affecting the management of GIS. It does not provide any clear approach to do the risk analysis.

Taking into account human factors during the risk analysis the level of risk change significantly, in some cases up to an order of magnitude going from acceptable risk to undesirable or in the worst case to unacceptable.

The results show that more exhaustive evaluation is necessary and that the interface between the operator and the equipment cannot be negligible.

When the risk level falls in the class unacceptable or undesirable some countermeasure is required.

To achieve useful results it could be necessary to apply some concept like “Safety Integrity Level”, which is currently only related to machinery but probably adaptable to high voltage equipment.

In the specific case of GIS some technical specifications exist (Terna, 2010) and gives some interesting guidelines that could be taken into account to improve the accessibility of the bays.

The results were discussed in a review meeting with operational personnel and the safety supervisor of the company interested in this issue. They approved and confirmed the problems highlighted by the analysis and will use them to try and identify feasible solution with the management.

Table.5: Table reporting an extract of the FMEA performed on the GIS

id	**Man-Machine function**	Failure mode	Causes	Consequences	L	C	R
6	**Visual inspections**						
6.1	**Take counter reading if cycles above 10.000 perform minor maintenance**	Operating cycle counter does not work	Operating linkage is loose or defective operating cycle counter is defective	Incorrect maintenance	B	III	2
		Operator can not see the counter	Awkward reachability	Incorrect maintenance			
6.2.1	Inspect cabinet(free of damages), check heater functions, verify ventilation opening allow free air movement, examine view windows must be clear of dust and moisture	Operator fail to make the checks	The window to be checked and the ventilation opening are not easily reacheable	Presence of moisture in the breaker can go undetected	B	II	1

References

Buakaew S., 2010, Reliability Centered Maintenance For Gas Insulated Switchgear Maintenance. Conference Proceedings CEPSI 2010, Taipei, October 24-28, Lecture TS1604.

CEI IEC 62271-202, 2006, High-voltage switchgear and control gear, European Committee for Electrotechnical Standardization, Brussels, Belgium.

CESI Report, 2005. Development of processing tools with a limited but significant data.

EN IEC 61508, 2010, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, International Electrotechnical Commission, Geneva, Switzerland.

IEC 61062, 2005, Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems. International Electrotechnical Commission, Geneva, Switzerland.

IEC 62271-1, 2007 High-voltage switchgear and controlgear - Common specifications. International Electrotechnical Commission, Geneva, Switzerland.

IEC 62271-202, 2006. High-voltage switchgear and control gear. International Electrotechnical Commission, Geneva, Switzerland.

IEC 62271-203, 2004. Gas-insulated metal-enclosed switchgear for rated voltages above 52 kV. International Electrotechnical Commission, Geneva, Switzerland.

IEEE, 2010. Gas insulated substation experience feedback, IEE/PES Substation Committee, <ewh.ieee.org/cmte/substations/sck0/wgk6/Documents%20Posted/2-1-2012/GIS%20Experience%20Feedback%2010-1-10.pdf>, Accessed 10/05/2012.

MIL-STD-882, 1993. System Safety Program Requirements, US Department of Defense.

Swain A. D., Guttmann H.E.,1983. Handbook of human reliability analysis with emphasis on nuclear power plant application (final report), NUREG/CR-1278, Washington D.C., United States.

Terna, 2010, Technical specifications- Prefabricated equipment with isolated metal closure with gas SF6 for ratings equal or higher than 140 kV.