METHODOLOGY FOR RISK-BASED CONFIGURATION CONTROL OF NUCLEAR POWER PLANT OPERATION

Antonio Torres Valle, atorres@instec.cu
Departamento de Ingeniería Nuclear, Instituto Superior de Tecnologías y Ciencias Aplicadas,
Ave. Salvador Allende, esq. Luaces, Quinta de los Molinos, Plaza, Ciudad Habana, Cuba

José de Jesús Rivero Oliva, rivero@con.ufrj.br
Departamento de Engenharia Nuclear, Universidade Federal do Rio de Janeiro,
Av. Horácio Macedo, 2030, Bloco G, Sala 201, Cidade Universitária, Ilha do Fundão, Rio do Janeiro, RJ, Brasil

Abstract. *The hazardous configurations control in Nuclear Power Plants is an application of a previous Probabilistic Safety Analysis (PSA). A more complete option would be the risk monitoring for the online detection of these configurations but expert personnel would be required to deal with the complexities of PSA and risk monitor. The paper presents a simpler but effective aproach: a method of configuration control, based on dependencies matrixes. The algorithm is included in a computer code called SECURE A-Z. The configuration control is carried out in a qualitative way, without previous PSA results and not using a Risk Monitor. The simplicity of the method warrants its application to facilities where these tools have not been developed, allowing the detection of hazardous configurations during operation and increasing plant safety. This configuration control system was implemented in the Embalse Nuclear Power Plant in Argentina. The paper shows the application of the algorithm to the analysis of a simplified safety system.*

Keywords*: configuration control, Probabilistic Safety Analysis (PSA), dependencies matrix, PSA applications, risk monitor*

1. INTRODUCTION

The configuration control is a recommended task for the safe operation of facilities with associated risk, essentially Nuclear Power Plants (NPP) (Samanta et al., 1994; Sam Sandani, 1996). This experience has been extended to others non-nuclear processes.

A dangerous configuration appears, in its most serious way, when all the redundancies of any safety system are affected simultaneously. In this case a critical configuration is formed as a result of the combination of unavailable equipments, constituting at least one Minimal Cut Sets (MCS) and determining a system fault state. But it is also very important to consider the cases when such combinations of equipment unavailability are close to any of the possible critical configurations. In such a case, a simple new failure or unavailability would lead to a critical state. In order to avoid these dangerous conditions, allowable outage time (AOT) are included as part of Plant technical specifications. AOT constitutes a limit for equipment downtimes when a NPP is in operation. It is a function of the safety systems redundancy (Samanta et al., 1994; US-NRC, 1994; US-NRC, 1993; Torres and Rivero, 2006).

In fact the random development of undetected dangerous configurations, sometimes critical, facilitates the initiation or progression of catastrophes, as it was in the case of the Three Miles Island accident (Torres and Rivero, 2006; Cox and Tait, 1998). The maintenance human error made on both auxiliary feedwater pumps facilitated the completion of a chain of events leading to the accidental sequence with reactor partial core melt, with serious consequences to the plant itself, as well as to the USA and other countries nuclear power programs.

Two of the most important applications of the Probabilistic Safety Analysis (PSA) are the configuration control tasks and the determination of redundancies AOT (US-NRC, 1994; US-NRC, 1993; Torres and Rivero, 2006; Cox and Tait, 1998). Many technical specifications are declared explicitly as parameters resulting from a previous PSA (Torres and Rivero, 2006; Cox and Tait, 1998; Fullwood, 2000; IAEA, 1992; US-NRC, 1994; US-NRC, 1993). Unfortunately, this type of technical specification is unrealistic for critical configurations because there are, in general, thousands or millions MCS describing all the possible cases. In fact, the configuration control specifications try to avoid only the most probable combinations.

Due to the various causes of unavailability (random failure, test or maintenance unavailability and equipment operational rotation) and the great quantity of equipments to be monitored in a complex facility, it is possible to overlook dangerous configurations. A team of safety specialists should compare plant configurations with PSA minimal cut sets to prevent critical or quasi-critical configuration occurrences, but this solution can not be implemented operatively due to the dynamic nature of NPP operation. An integral solution to this problem would be the use of a Risk Monitor (Torres and Rivero, 2006; Kafka, 2008; Salomón et al., 2010) supported on the PSA results (Fullwood, 2000;

IAEA, 1992; US-NRC, 1985; Smith, 2001). This type of tool can monitor on-line the existing combinations of equipment unavailability and advice immediately to the operators about dangerous situations. A risk monitor (Torres and Rivero, 2006; Kafka, 2008; Salomón et al., 2010), with capacity to update the Boolean reduction process and reconfigure the PSA minimal cut sets list dynamically, is able to supervise millions of dangerous configurations. It includes the reevaluation of risk main contributors and global risk for specific operative situations, as well as a comparison with the respective baseline values, to support decision making.

The previously described alternatives require personnel with PSA expert knowledge (Fullwood, 2000; IAEA, 1992; US-NRC, 1985; Smith, 2001; Torres et al, 2010) and/or a costly risk monitor (Torres and Rivero, 2006; Kafka, 2008; Salomón et al., 2010), which are important obstacles to solve this complex problem effectively.

Consequently, the main objective of the present paper is to demonstrate an alternative method for hazardous configuration control (Torres et al., 2011; Torres and Perdomo, 2010) in NPP, based on dependencies matrixes and without previous PSA or Risk Monitor availability.

2. CONFIGURATION CONTROL THROUGH DEPENDENCIES MATRIX

The configuration control in NPP requires, in general, a previous PSA. Consequently, any offline configuration control would require the experts to understand and apply the result of PSA (IAEA, 1992; Torres et al., 2010). A more effective way of implementing the risk based control would be an upgrade of the existing PSA, transforming it into a Living PSA (Torres y Rivero, 2006) that assures a continuous update process of the risk analysis. An advance tool like a Risk Monitor would allow an online risk surveillance of the facility (Kafka, 2008; Salomón et al., 2010). Taking into account the associated complexities of the risk analysis (high volume and quality assurance of the tasks, long times for the study execution, dependencies of high level informatics tools and necessity of specialized personnel and others) (IAEA, 1992; US-NRC, 1985, Torres et al, 2010) and the more simple structure of the dependencies matrixes, was developed an informatics code (SECURE A-Z) (Torres et al., 2011; Torres and Perdomo, 2010) to trace the hazardous configuration of equipments with qualitative and practical focus and more useful to the unprepared operators in this expert area of knowledge.

The bases of this method are two kinds of tables: the systems failure criteria table (systems table) and the systems dependencies table (dependencies table), and the algorithm for tracing the dependencies and classification of the final state of the systems after the postulation of any equipment outages configuration. The first kind of table contains the failure criteria of the monitored technological systems. The second table describes in an analytical way, the dependencies between equipment, subsystems and interfaces supporting the function of the monitored systems.

The tracing algorithm of dependencies was structured as a close cycle which identifies the original affected front line or interface equipments and traces the existing relations between different parts of the systems, to evaluate the resulting effect at system level, categorizing the final state of the monitored systems using a qualitative scale of six classes: fault, low degraded, medium degraded, high degraded, fail safe or spurious alert.

2.1 Illustrative example. Input data

Figure 1 shows an illustrative technological system.

The system SS is composed by two lines of 100 % capacity to cool the point A. Both lines take water from the common tank SS-TK1. Each line (line SS11 for example) contains a pneumatic valve (SS-VA1), a check valve (SS-VR1) and a motorized pump (SS-PM1). The pneumatic valve depends on the pneumatic control subsystem, whose design is based on fail safe principle. This subsystem is integrated by the solenoid valve (SS-VS1) and air tank (SS-TA1). On other hand, the motorized pump (SS-PM1) depends on the electrical, control and oil cooling interfaces. The electrical subsystem includes a bus (SS-BR1), a circuit breaker (SS-KA1) and a transformer (SS-TR1). The control system is integrated by a control relay (SS-ER1), a battery (SS-BT1) and two redundant starters: one logic panel (SS-PA1) and one push button (SS-PB1). Finally, the oil cooling subsystem contains an oil pump (SS-BA1) and a heat exchanger (SS-IT1).

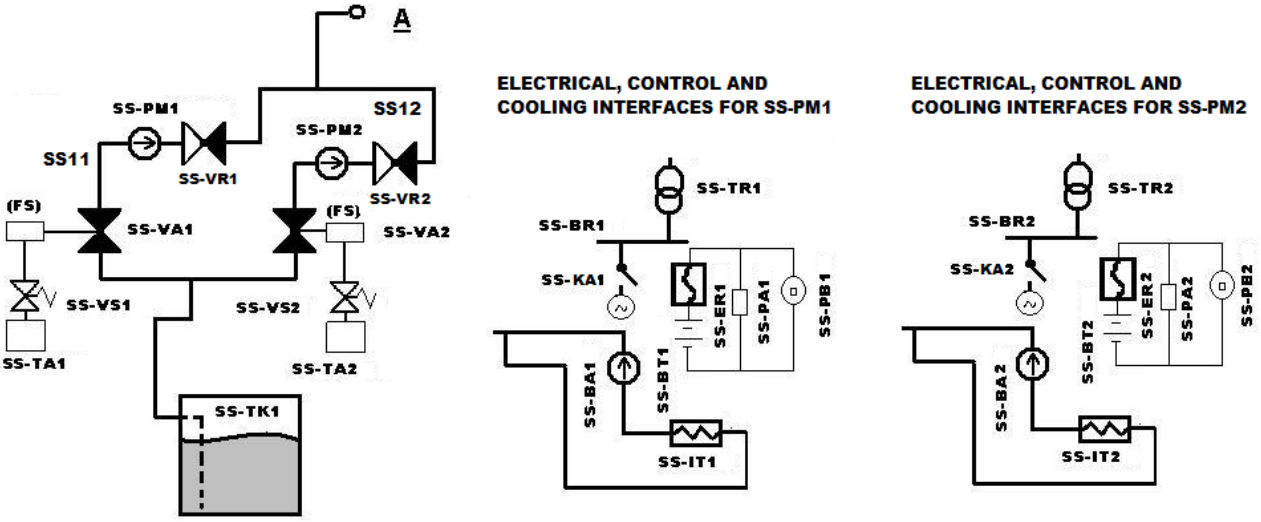

Figure 1. Illustrative Technological Safety System SS

The preparation of a dependencies matrix is a common task in PSA. This kind of task allow the systematically knowledge of the interfaces of the systems included in the risk study. For example, Tab. 1 presents the dependencies matrix for the system SS.

Table 1. Dependencies Matrix of system SS

Equipments	Interfaces		
	Oil cooling	**Electrical**	**Control**
SS-PM1	SS-BA1; SS-IT1	SS-KA1; SS-BR1; SS-TR1	SS-ER1; SS-BT1; SS-PA1, SS-PB1
SS-PM2	SS-BA2; SS-IT2	SS-KA2; SS-BR2; SS-TR2	SS-ER2; SS-BT2; SS-PA2, SS-PB2
SS-VA1			SS-VS1, SS-TA1
SS-VA2			SS-VS2, SS-TA2

The systems table includes a descriptive column “System”. The column “Code” assigns a string that will serve as a system identifier for the tracing algorithm. Finally, the column “Criteria” contains the parameters F (Faults), R (Redundancies) and keyword (criteria). These parameters are joined in a structure of the type “F/R keyword”, where F represents the quantity (2) of redundancies R (2) with keyword criteria (LIN - line) that satisfy the fault characteristic for the system.

Table 2 shows the systems table for the system SS.

Table 2. Systems table for system SS

Nu	System	Code	Criteria
1	Safety System	SS1	2/2 LIN

The dependencies table contains several columns. The column “System” is used to identify the monitored systems. The rows corresponding to the column “Criteria” shows a set of short codes representing the success criteria of the systems redundancies. The column “Equipment” contains the interconnections between the different parts of the system. Finally, the dependencies (located in columns DEP..) shows the structure of each part (components, subsystems, interfaces) of the system. Table 3 shows a fragment of the dependencies table for the system SS.

Table 3. Fragment of dependencies table for system SS

Nu	System	Red.	Criteria	Equipment	DEP1	DEP2	DEP3	DEP4	DEP5	DEP6
1	SS1			@SS1	R1:@SS11	R2:@SS12				
2	SS1		LIN	@SS11	@SS-PM1	@SS-VA1	SS-VR1	SS-TK1		
3	SS1		LIN	@SS12	@SS-PM2	@SS-VA2	SS-VR2	SS-TK1		
4	SS1			@SS-PM1	SS-PM1	SS-BR1,SS-KA1	SS-ER1,SS-BT1	SS-BA1,SS-IT1,	R1:SS-PA1	R2:SS-PB1
5	SS1			@SS-PM2	SS-PM2	SS-BR2,SS-KA2	SS-ER2,SS-BT2	SS-BA2,SS-IT2,	R1:SS-PA2	R2:SS-PB2
6	SS1			@SS-VA1	SS-VA1	FS:SS-VS1	FS:SS-TA1			
7	SS1			@SS-VA2	SS-VA2	FS:SS-VS2	FS:SS-TA2			

Also, the dependencies table use some colors and characters to remark important attributes of the systems components, for example, the use of green cells with characters “R#:” to represent redundancies, and blue cells with characters “FS:” to represents fail safe structures.

2.2 Tracing Algorithm. The code SECURE A-Z

The tracing algorithm was implemented in the computer code SECURE A-Z (Torres et al., 2011; Torres and Perdomo, 2010). It consists of a recurrent cycle that determines the primary impact of all existing unavailability combinations and their subsequent traces until the dependencies propagation reaches the system level and the consequences evaluation is completed for all the structures considered in the analysis, including the categorization of the systems final states.

Figure 2 shows the algorithm to trace the dependencies of the systems.

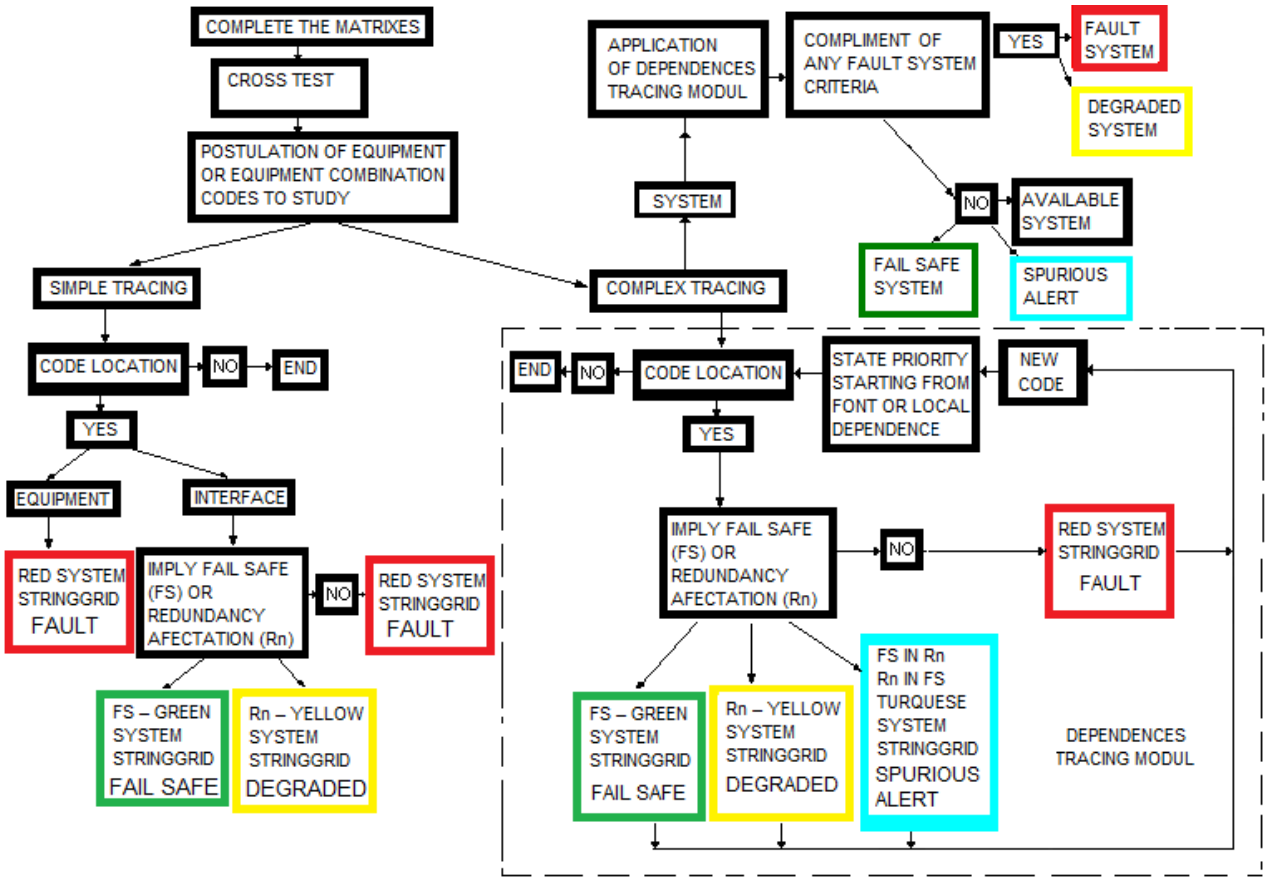

Figure 2. Tracing Algorithm implemented in the computer code SECURE A-Z

The left side of Fig. 2 represents the initial simple tracing process that implies the detection of the affected original equipment and the determination of the corresponding operational state (fault, degraded or fail safe) at the level of the affected rows in the dependencies matrix. The right side of Fig. 2 corresponds to the tracing process of the initial impacts throughout the entire matrix until the systems level is reached. The process includes the detection of new equipment unavailability couplings at upper levels and the conservative deduction of the operational states corresponding to these intermediate levels. Finally, the algorithm establishes the classification of the safety condition state at the system level, using one of the six previously defined classes.

3. MAIN RESULTS

The computer code SECURE uses simple and familiar codes of colors to illustrate the state of the different systems included in the matrix as a consequence of a single or multiple component failure or unavailability. This characteristic enhances operators' acceptance, in contrast with the traditional rejection to PSA and Risk Monitors, due to the lack of understanding of "probabilistic language".

The next example illustrates the capacity of the computer code SECURE for configuration control problems. The hypothetical degraded configuration is the unavailability combination of the equipments SS-VA2 and SS-PA1. In this case, the algorithm determines the loss of one of the control redundancies of pump SS-PM1 from line SS11, due to the unavailability of the logic panel SS-PA1. The second line SS12 is in a fail state condition, which arises directly from the failure of pneumatic valve SS-VA2. Finally, the system SS is categorized in a **high degraded** state because of the full unavailability of one line (SS12) and the degraded state of the other (SS11).

Table 4 shows the result of the tracing process for the system SS after the input of the configuration equipment. The lines show, in an illustrative way, the location of the originally unavailable components and the traces propagation to the following levels of the matrix until the final state of the system SS is identified as "high degraded". The colored lines also simulate the dependencies propagation process through different levels.

Table 4. Tracing process starting from the unavailability of the equipments SS-VA2 and SS-PA1

	Nu	System	Red.	Criteria	Equipment	DEP1	DEP2	DEP3	DEP4	DEP5	DEP6
HIGH DEGRADED	1	SS1			@SS1	R1:@SS11	R2:@SS12				
DEGRADED	2	SS1		LIN	@SS11	@SS-PM1	@SS-VA1	SS-VR1	SS-TK1		
FAULT	3	SS1		LIN	@SS12	@SS-PM2	@SS-VA2	SS-VR2	SS-TK1		
DEGRADED	4	SS1			@SS-PM1	SS-PM1	SS-BR1,SS-KA1	SS-ER1,SS-BT1	SS-BA1,SS-IT1,	R1:SS-PA1	R2:SS-PB1
	5	SS1			@SS-PM2	SS-PM2	SS-BR2,SS-KA2	SS-ER2,SS-BT2	SS-BA2,SS-IT2,	R1:SS-PA2	R2:SS-PB2
	6	SS1			@SS-VA1	SS-VA1	FS:SS-VS1	FS:SS-TA1			
FAULT	7	SS1			@SS-VA2	SS-VA2	FS:SS-VS2	FS:SS-TA2			

The input configurations identified by the computer code SECURE match perfectly with the MCS determined by the PSA code for Maintenance Applications MOSEG (Torres and Rivero, 2006). Table 5 shows the comparisons for some input configurations.

Table 5. Comparisons between input configurations identified in SECURE and MCS obtained by MOSEG

Input Configuration in SECURE	Some MCS (using code MOSEG) associated with the input configuration
SS-TK1	SS-TK1.T
SS-PM1, SS-PM2	SS-PM1.S * SS-PM2.S , SS-PM1.S * SS-PM2.R , SS-PM1.R * SS-PM2.S
SS-VA1, SS-VA2	SS-VA1.O * SS-VA2.O
SS-ER1, SS-VA2	SS-ER1.F * SS-VA2.O
SS-PB1, SS-PA1, SS-VA2	SS-PB1.F * SS-PA1.F * SS-VA2.O

The potentialities of the computer code SECURE A-Z has been confirmed through its application to real cases of very high complexity, performing configuration control tasks in the Argentinean NPP Embalse for 21 technological systems with more than 1600 associated equipment and interfaces (Torres and Perdomo, 2010), and for the Center of Isotopes in Cuba, for 5 technological systems and near to 400 related equipment and interfaces.

The application of this methodology has been extended to qualitative safety studies, starting from the characterization of the safety basic principles by means of dependencies matrix (Torres et al., 2011) and with the

incorporation of the quantitative magnitudes to analyze the random combination of outages in the long period of operation of the facilities.

4. CONCLUSIONS

The dependencies matrix method was implemented in the computational tool SECURE A-Z to carry out very complex tasks like the configuration control. This tool allows a qualitative way of configuration control, more familiar to the operators, without using previously developed PSA models. The possibilities of the computer code include the predictive and corrective studies of any unavailability configuration. The capacity of SECURE A-Z has been proved in real complex cases.

The proposed algorithm could be considered also a previous step to the PSA application or a full scale Risk Monitor implementation. While a PSA study is not available, this simplest but effective algorithm, implemented in a user-friendly PC environment, can improve considerably the NPP configuration control.

5. REFERENCES

Samanta, P.K., Mankamo I.S., Vesely, W.E., 1994, Handbook of Methods for Risk-Based Analyses of Technical Specification, U.S. Nuclear Regulatory Commission, Washington DC, p. 3-1 to 3-22, p. 5-1 to 6-18. NUREG/CR-6141, BNL-NUREG 52398

Sam Samdani, G., 1996, Safety & Risk Management Tools & Techniques in the Chemical Processes Industry. New York: McGraw Hill. 1996. p. 57-66, p. 67.

US-NRC. 1994, Commission Briefing Proposed Rulemaking. Technical Specifications. 10 CFR 50.36, USA: CFR.

US-NRC. 1993, Maintenance Rules. 10 CFR 50.65. USA: CFR.

Torres, A., Rivero, J.J., 2006, Mantenimiento Orientado a la Seguridad, Primera Edición. Ciudad Habana: CUBAENERGIA. 442 p. ISBN 959-7136-10-4. p. 139, 338, 408, 413.

Cox, S., Tait, R., 1998. Safety, Reliability and Risk Management: an integrated approach. Second Edition. Oxford: Butterworth - Heinemann. 325 p. ISBN 0-7506-4016-2. p. 290 – 315.

Kafka, P. 2008, Probabilistic Risk Assessment for Nuclear Power Plant. Handbook of Performability Engineering, London: Springer. ISBN 978-1-84800-130-5. p. 1179-1192.

Salomón, J., Perdomo, M., Rivero, J.J., Sánchez, D., Frías, D., 2010, Monitoracao Contínua da Confiabilidade e Riscos em sistemas integrados e distribuídos, Rio Oil & Gas Expo and Conference 2010, Río de Janeiro, 13 de Setembro de 2010.

Fullwood, R.R. 2000. Probabilistic Safety Assessment in the Chemical and Nuclear Industries. Second Edition. Oxford: Butterworth - Heinemann. 514 p. ISBN 0-7506-7208-0. p. 97 – 122.

IAEA. 1992. Procedures for Conducting PSA in NPP. Safety Series No. 50-P-4.

US-NRC, 1985. Probabilistic Safety Analysis Procedures Guide. NUREG/CR-2815.

Smith, D.J., 2001. Reliability, Maintainability and Risk. Practical Methods for engineers. Second Edition. Oxford: Butterworth - Heinemann. 335 p. ISBN 0-7506-5168-7. p. 128 – 144.

Torres, A., Perdomo, M., Fornero, D., 2010, Aplication of Realibility Centered Maintenance of Nuclear Power Plant Embalse, Revista Nucleus, No. 47, pag. 24 – 29, ISSN 0864-084X (web: http://scielo.sld.cu/scielo.php?pid=S0864-084X2010000100002&script=sci_arttext)

Torres, A., Perdomo, M., Rivero, J.J., 2011., Computerized matrix of safety basic principles: a useful alternative for their learning and application, Revista Ingeniería Mecánica, Vol 14, No. 3, ISSN 1815-5944, p. 221-229 (web: http://revistascientificas.cujae.edu.cu/Revistas/Mecanica/Vol-14/3-2011/06_2011_03_221_229.pdf)

Torres, A., Perdomo, M., 2010. Control of dangerous configurations in Nucler Power Plants througth the dependences matrixes, Revista Nucleus, No. 47, pag. 8 – 15, ISSN 0864-084X (web: http://scielo.sld.cu/scielo.php?pid=S0864-084X2010000100002&script=sci_arttext)

6. RESPONSIBILITY NOTICE

The authors are the only responsible for the printed material included in this paper.