METHOD FOR MONITORING AND REDUCING THE ACCIDENTS RISK IN POWER UNITS

Gheorghe FLORESCU[1], Valeriu Nicolae PANAITESCU[2]

The paper presents a specific method to integrate and use the deterministic and probabilistic models in a process and risk monitoring system, in order to monitor, analyze and improve the reliability, availability, safety of the power systems and to reduce risk of accidents. In the paper are also specified the applications of probabilistic and deterministic modelling to perform online and offline monitoring of process, reliability, unavailability, safety or risk associated to the analyzed system. Also in the paper is presented a case study for use of probabilistic modelling in test intervals optimizing in technological systems.

Keywords: power plant, risk monitoring, online data acquisition and intelligent components.

1. Introduction

The evaluation of risk of accidents for the industrial facilities is intended to improve the safety, reliability, availability of structures, systems and components (SSCs), to guarantee the security of operational personnel and to harmonize and preserve the environment conditions.

One important source of uncertainties, during the process of modelling and monitoring of SSCs safety and reliability, is reliability data. Improved techniques and methods for collection, analyzing and processing of data could reduce or optimize the uncertainties factors.

Efficiency of on-line data acquisition is in continuous progress this permitting the SSCs model updating in real time.

One technique to make a risk monitor is based both on hardware and software that use probabilistic and deterministic models. Computers - and implicitly computer codes - have to permit and facilitate the development and use of modelling tools and techniques. To process large probabilistic models the computer codes must be specially designed, developed, tested and validated and also must have rapid computation characteristics. For such models the effects of process or environmental conditions could be incorporated either as initiated

[1] Eng., Reactor Safety Department, INR, Institute for Nuclear Research, 15400, Pitesti-Mioveni, Romania, e-mail: gheorghe.florescu@nuclear.ro.
[2] Prof.., University POLITEHNICA of Bucharest, Romania.

events or by the effect of process or environmental parameters to the structures, systems or components (SSCs) operation.

During the NPPs operational behaviour surveillance, acquisition of reliability data or reading of process or reliability parameters are important activities with the goals to determine the causal chains of an accident or undesirable events that could be viewed as a sequence "root" cause, also could appear one or more "intermediate" causes [3], and finally the undesirable event (accident/incident). The intermediate causes many times lead to undesirable events that are called proximate causes of the accident and also conditions identifiable as leading to failures or accident. In some cases proximate causes are symptoms of the actual cause.

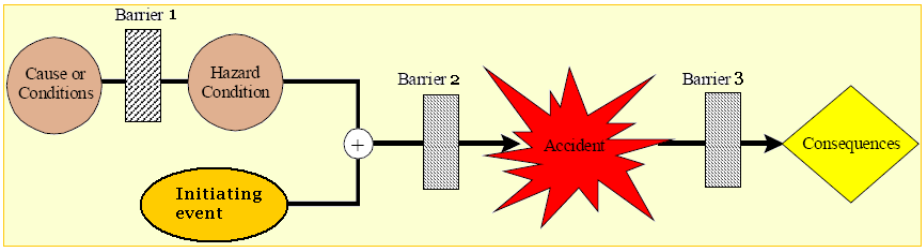

Fig. 1. Causal Chain and Role of Hazard [3]

A hazard condition [3] is an event, condition or cause, in a causal chain that needs an activating, conditioning or trigger event to generate failure or accident in a system or power plant.

Collecting and processing the data [4], in order to make them usable for the R&D purposes and also to monitor the reliability performance, is a long process, failure data accumulate too slowly and doesn't indicate accurately the actual state of performance.

Bayesian methods could be used to estimate data by prior distribution, in fact estimating the parameters that don't change, more easy been to use prior that is proportional with specific reliability parameter.

For common applications for data updating could be considered the following priors [4]:

- *Industry prior,* knowing the past performance of similar facilities (*realistic*, not diffuse enough);
- *Jeffrey's non-informative prior* (*very diffuse*, unrealistic);
- *Forced non-informative prior* (*diffuse*, not flexible);

Good Bayesian practice involves looking [4] at the data to make sure that the observations are consistent with the prior belief otherwise probably is an error to use the data for prior updating.

To eliminate the above issues *the data could be directly collected by* using of on-line data acquisition devices based on intelligent and smart sensors and appropriate processing tools and software. Some computer codes use compound documents that contain various types of information.

2. Methodology used for online risk monitoring system development

There are nuclear facilities or industrial systems with undesired consequences in case of accident (or initiating events). During stress conditions, the time to take correct decisions is difficult to be low. This situation could be changed by taking automatically the data. Also by using automatic data acquisition technique the configuration of a system could be changed as desired depending of the facility operational state, of the process or of the environmental parameters. Also by using this data collection mean specific data for facility's components is made available.

Several times in the power unit process of operation, as a result of abnormal events occurrence, the facility operational personnel has short time for decision and intervention in order to mitigate the initiating events, to prevent the components failures and to minimize the event consequences.

The evaluation of risk associated to the process or environmental conditions effects is very important in such cases to help decision making and to reduce undesired consequences.

The main methodology that is used for modelling of system design and behaviour during normal or abnormal conditions is *probabilistic risk assessment* methodology with support of deterministic safety studies. This methodology consists mainly of development of event tree and fault trees approach. Several key activities have to be performed in order to reach the main goals of this methodology and to obtain useful results that could be interpreted and used for improvement of equipment reliability or availability. Specific or generic data - based on reliability parameters - is also essential in reaching the PSA study scope. By using on-line reliability data acquisition, based on intelligent and smart sensors, several analysis tasks could be synchronized, harmonized, optimized or made effective and efficient.

Time for data acquisition, processing, transfer and implementation, time to take decision for operation and costs of research activities and overall activities are the main resources that could be reduced by using the new data acquisition technique.

Specific models optimization could also be done.

By using on-line risk monitors could be also assured the *prevention of evolution of severe or major accidents after initiating events occurrence,*

prevention of making wrong design changes and treatment of wrong accident sequences as dominant.

For the efficient online risk monitor are also used intelligent components that are based on smart and intelligent sensors, transmitters and processing equipment.

An *intelligent component* is a component that has associated one or many sensors having direct connections to the intelligent electronic circuits (devices) permitting the acquisition and processing of data and information and also giving some commands and information to other devices for execution or to permit taking of decision.

The data acquisition equipment could consist of signal sensors that allow reading of data, data acquisition cards or advanced data acquisition modules or systems.

The online data acquisition is possible to be undertaken if exist the component that generate the event, the component's associated sensor that „*observe*" the event occurrence and an information or data transmission channel - to the system of collecting, processing and storage of data.

The elements of intelligent components are:

- *The component that is under surveillance;*
- *The sensor that „observes" the evolution or change of the process parameters, of the process itself and of the component operating state or failure state;*
- *The communication channel between the sensor and the data acquisition, processing and storage intelligent device;*
- *The data acquisition, processing and storage intelligent device.*

A simple schematic of an intelligent component is presented in the picture below.

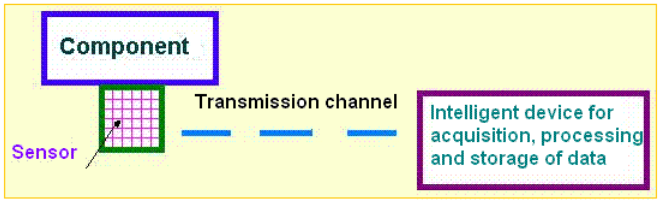

Fig. 2. The elements of a typical intelligent component

The solutions that must be implemented in a prototype of risk and process monitor, in order to eliminate the above negative aspects - to have such technique for risk and process monitoring and to make it functional the following changes - must be performed in a common risk and process monitor are: *monitored facility configuration change* in order to permit monitoring of component's states (the major modification is the facility of smart or intelligent sensors for monitoring the

component's states and the facility's processes or failure parameters); *providing of devices for specific data transmission, acquisition and processing (*to permit data use in facility modelling)*; providing of automatic updatable fault tree and event tree models* (to permit reconfiguration of them in case of system hardware reconfiguration - in case of components failure); *possibility for system reconfiguration presentation* (by use of interactive system schematic on computer); s*pecific software development* (to link all the risk monitor pieces).

3. Main risk and process monitor technique description

A definition of risk based management is that the power system operation and the total risk of associated consequences are maintained under acceptable levels.

A risk monitor - as a hardware - has the following components:

- *A specifically configured computer (*for software processing and interfacing with the data acquisition equipment)*;*
- *Data acquisition equipment (*a simple or a complex device)*;*
- *Support equipment;*
- *Specific smart and intelligent sensors (*collect data and information from the technological process).

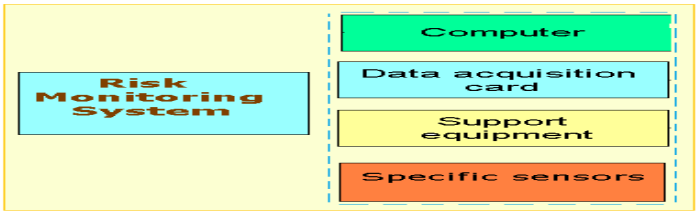

Fig. 3. Specific hardware components used for online monitor development

As integrated equipment, the online risk monitor (ORM) consists from software, hardware, data acquisition equipment and, in some cases, specific calibration components.

Specific software links the monitoring system components in order to create the on-line risk monitor structure.

The characteristics the software for ORM permits:

- *Developing, editing, modifying and processing of analyzed facility models;*
- *Data acquisition and processing;*
- *Results representation and processing;*
- *Facility schematic interaction with data from their components.*

In table 1 is presented, as an example, typical data from the assisted facility by means of appropriate intelligent sensors, data acquisition models and processing of the data.

Table 1

Specific typical data obtained by using the acquisition module

Time [s]	Parameter 1	Parameter 2
0.00	4	0.047
0.05	6	0.071
0.10	9	0.106
0.15	12	0.141
0.20	14	0.165
0.25	17	0.200
0.30	20	0.235
0.35	22	0.259

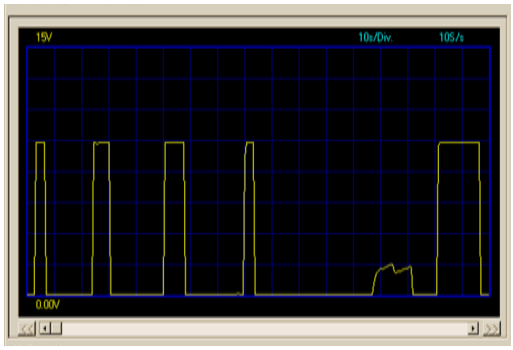

Fig. 4. Example ORM display with events representation associated with a monitored component

The software that is used to integrate the risk monitor components communicates with a specific acquisition module, with many channels, for technological process signals monitoring and computing. The signals collected from the facility operating process are computed by data acquisition module and converted in specific information and data that can be used for the facility reliability, availability and risk or safety calculation.

3.1 The modifications that are necessary to be implemented in the specific facility that would be evaluated

Having a specific industrial facility that must be monitored, in order to be improved (looking to the operation, maintenance, repairing or testing) this facility - or industrial system – have to be modified in order to permit the montage of the signal sensors. In the industrial facilities is used different type of sensors, depending of the facility's components. But looking to these sensors not all of them are appropriate to be associated to a monitored component. In order to perform this association have to make a preliminary analysis looking to the specific component (that have to be monitored) type, operation parameters, failure

modes and other factors. For instance such sensors could be associated as in table below.

Table 2

Correspondence between component with failure mode and associated sensor

Component type	Failure modes	Type of sensors
Mechanical valves	*fail open, fail closed*	*contact switches*
Pressure relief valves	*fail open, fail closed*	*pressure sensors*
Pumps	All	*pressure sensors*
Electrical motors	All	*electrical sensors*

Data from sensors is processed and transmitted to the facility models to be included for processing of these models. By using such sensors could also be monitored the process or environmental parameters that influence the facility operational behaviour.+

In the modelling process, the data that is used could be obtained from specific or generic databases. By using the online data acquisition and processing, the data for fault tree quantification could be automatically updated and more specific for the analyzed facility.

On the industrial market it exist several data acquisition products, a typical acquisition module is presented in the installation presented in the picture below.

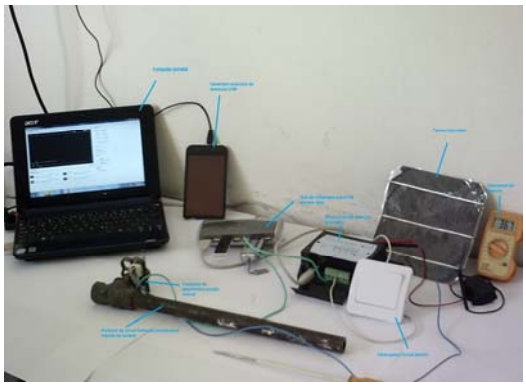

Fig. 5. Online data acquisition installation that uses specific input signal channels

Such online data acquisition devices process specific signals (see above figure) and convert them in appropriate information or data that can be used in specific modelling and surveillance applications (PSA models).

3.2 Basic facility models changing in order to develop the online risk monitor

In the present approach, to develop an ORM, by using PSA methodology, the basic models are event trees and fault trees. To process them - by using specific computer codes - are needed reliability data and parameters.

There are two major adaptations that have to be satisfied by the fault tree models in order to permit ORM use. One modification is the direct connection between the sensor and reliability data file in order to update de date when changed. Other major modification is for the fault tree that needs to change structure depending of the component failure mode or availability. The fault tree changing must be done in such a manner to permit that input data to be easily modified and used and to reflect the new system configuration. In this respect to use switch events could be a solution. Such options that include switch events automatic transfer of component as failed or available lead to dynamic fault tree structure. In the picture below is presented how could be modify a fault tree structure in order to permit facile updating based on components availability. So in the fault tree will be inserted an event that could be included or not the event is transformed in "AND" gate having as inputs the original event and a trigger event that depends of the component' associated sensor state. For the possibility to reflect that the event occurred the "decision" event value is 1 otherwise this value is 0 and the event will not be considered.

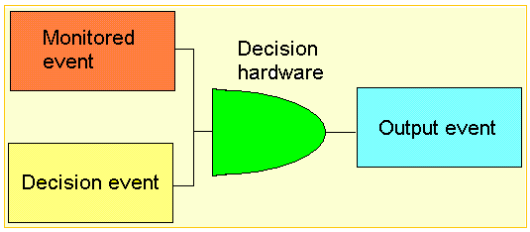

Fig. 5. Modification of the fault tree logic to permit on-line risk monitoring.

If the trigger event appears the probability will be 1 otherwise 0.

An important advantage of the on-line risk monitor is also the possibility to present the new facility configuration (*or the reconfiguration of the facility*) by providing to the overall monitoring system interactive images or schematics for the facility, where the component failure states appear immediately as it appear.

3.3 Use of process and risk monitors in management of SSCs operational activities. Harmonizing the power unit's operational activities.

Coordination of the important activities that have to be performed during facility operational actions, associated to the SSCs that belong to the power units, mean to look to different goals.

Hydraulic circuits consist especially from mechanical components that periodically need maintenance. For maintenance purposes, in the redundant trains the policy to put under maintenance one train must be such way assured to permit operation as required and performing of the necessary circuit functions. The line

that is under maintenance must be notified and alerted to prevent running hydraulic line to be inadvertently take-off from operation. A common mistake in circuits that have groups of two 2x100% redundant lines is to stop the line in operation due to planned maintenance reasons when the other line failed. Many times this could be an inadvertent action due to the fact that circuit function assurance doesn't permit interruption.

Let's consider a mechanical hydraulic circuit with 2x100% pumping line each one in running, the other in operation. The main function of the circuit must be assured without interruption otherwise the consequence could be disastrous. To prevent catastrophic damages must take other actions that require enough time, for instance for pressure decrease. In this case the maintenance must be carefully planned to be sure that the circuit function is assured without interruption.

For the presented case the important tasks are to have the required redundancy, the adequate operation and maintenance procedures.

So for success criterion this could be changed to 3x50% during the period in which the standby line is in maintenance.

A 2x100% success criterion is adequate for process systems where the circuits and SSCs are not safety related.

Selection of the success criteria must be in accord with the level of severity for circuit running interruption. Adequate success criteria could be 4x33.3% or more.

Harmonizing the activities for the line in maintenance means often optimization and synchronization. Several maintenance activities must be synchronized to permit parallel maintenance activities to reduce the time in which the standby line is unavailable.

Ageing modelling (Living PSA) during equipment operation is also possible to be done in order to describe the failure rates as function of time, to use of a model that take into account SSC not restoration due to degradation factor and to verify the ageing level imposed by a parameter.

To determine ageing state in a system could be considered different models used for failure rates representation, the simplest is the linear one presented below (1).

$$\lambda(t) = \lambda_0 + \alpha(t) \cdot (t - T_{POT}) \tag{1}$$

λ_0 is the failure rate specific to the initial state of SSC, $\alpha(t)$ is a factor that describe the speed with which the ageing happened.

$$\alpha(t)\begin{cases} 0 - t \le T_{POT} \\ a - t > T_{POT} \end{cases} \tag{2}$$

Ageing process lead to degradation of SSC characteristics and properties related to engineering, control systems and equipment relevant for the power plant

operation, specifications and documentation, personnel involved in the power plant operation.

4. Example of using a probabilistic model to evaluate the reliability parameters for hydraulic circuits

In the figure 6 below is presented a demonstrative system consisting of two hydraulic circuits (or two subsystems or one active system and one passive system). This example is presented to demonstrate the use of probabilistic modelling technique - associated with online data acquisition - in optimization of reliability parameters.

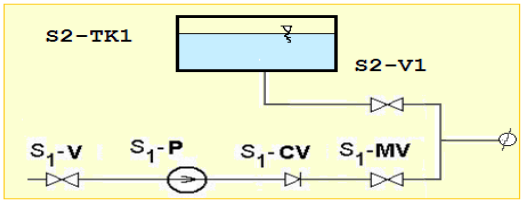

Fig. 6. Schematic of the hydraulic circuit (redundancy with diverse passive components).

An efficient method to increase the reliability of a hydraulic circuit is to replace the active components by reliable passive components in redundant diverse trains. In such case the frequencies of the initiating events decrease, also decrease the failure probability of the hydraulic circuit.

The storage tank S2-TK1 could be supplied with water from independent sources or by means of the S1 hydraulic circuit, of which flow and pressure characteristics are larges in order to permit the supply of TK1 tank. TK1 capacity is sufficient to permit loads supply on a period such as the CH S1 components are in repairing.

Tables 3 and 4 below presents the results obtained for the probabilistic evaluation of S1 and S2 logical models.

Table 3

Reliability data specific to a hydraulic circuit with serial components and TK as redundancy

Basic event	Lambda (events per 1000 years)	Mission time (days)	Test interval (days)	MTTR (hours)	Unavailability
/S1//CV//M/FC/	1.17	-	-	48	0. 0000064
/S1//MV//M/FC/	17.75	-	-	72	0.000146
/S1//P//M/MR/	2730	-	-	48	0.0147
/S1//V//M/FC/	0.2	-	-	48	0.0000011
/S2//TK/01/T/EL /	100	-	31	150	0.006
/S2//V/1/Q/FC/	100	31	-	-	0.00846

Table 4

Main contributors of top event (value of $2.147 \cdot 10^{-04}$)

MCS	Name	Value	Relative contribution
0	/S1//P//M/MR/ /S2//V/1/Q/FC/	$1.25 \cdot 10^{-04}$	58.1 %
1	S1//P//M/MR/ /S2//TK/01/T/EL/	$8.78 \cdot 10^{-05}$	40.9%
2	/S1//MV//M/FC/ /S2//V/1/Q/FC/	$1.23 \cdot 10^{-06}$	0.57%
3	/S1//MV//M/FC/ /S2//TK/01/T/EL/	$8.69 \cdot 10^{-07}$	0.43%

That top event value means a large difference like 0.934 initially value, that means a high reliability of group of hydraulic circuits. The two HCs were considered as 2 x 100% redundancy.

The assessment of the occurrence frequency of the initiating event "*Loss of water supply to the loads*" by using the same failure rates for the hydraulic circuits lead to the value of 3.96 events per 100 years, this is very close to the required failure criterion.

Table 5

Failure frequency assessment (top event value 39.6 events per 1000 years)

MCS	Name	Value	Relative contribution
0	/S1//P//M/MR/ /S2//V/1/Q/FC/	23.1	58.36%
1	/S1//P//M/MR/ /S2//TK/01/T/EL/	16.3	41.05%
2	/S1//MV//M/FC/ /S2//V/1/Q/FC/	0.15	0.33%
3	/S1//MV//M/FC/ /S2//TK/01/T/EL/	0.106	0.22%
4	/S1//CV//M/FC/ /S2//V/1/Q/FC/	0.001	0.025%
5	/S1//CV//M/FC/ /S2//TK/01/T/EL/	0.007	0.0176%

In the above example if the test interval is decreased to 15 days this will lead to a failure probability of $1.82 \cdot 10^{-04}$ and a failure frequency of 3.36 events per 100 years, this confirming the initial technical specification.

For the standby HC is estimated the "*on demand*" unavailability by using the formulas (3), (4), (5),

$$P = \frac{\lambda \cdot T_i}{2} \qquad \text{(F1)} \qquad (3)$$

$$P + Q = \frac{\lambda \cdot T_i}{2} + \lambda \cdot MTTR + \frac{t}{T_i} \qquad \text{(F2)} \qquad (4)$$

$$Q = \frac{t}{T_i} \qquad \text{(F3)} \qquad (5)$$

In such a way could determine, on comparative basis, the reliability parameters (in this case the test interval and the repair times). To determine the test interval are used F1 and F2 formulas.

In the situation of the estimation of the unavailability given by the operation stop (or removing from standby state) for repairing, maintenance or testing, the testing time – in this case t – could be not greater then repair time, in the situation when is identified a component which is found as fault when tested, is then repaired, tested again (is the most defavorable situation that could appear at a component test).

Considering that *t = MTTR this permits also the determination of the repair time and testing time. In the table 6 is presented a single component, the storage tank TK1 with associated activity, duration, service interval and activity type.*

Table 6

Component specific activity for an analysed hydraulic circuit

Equipment	Activity	Duration [h]	Service interval [days]	Activity type
S2-TK1	Testing of S2-TK1 tank integrity and function	4	31	Testing

Table 7

Results for determination of the test interval

T [days]	F1	F3 [t = 5 hours]	F3 [t = 20 ore]
1	0.055	0.208	0.833
2	0.110	0.104	0.417
4	0.219	0.052	0.208
8	0.438	0.026	0.104
15	0.822	0.014	0.056
31	1.000	0.007	0.027

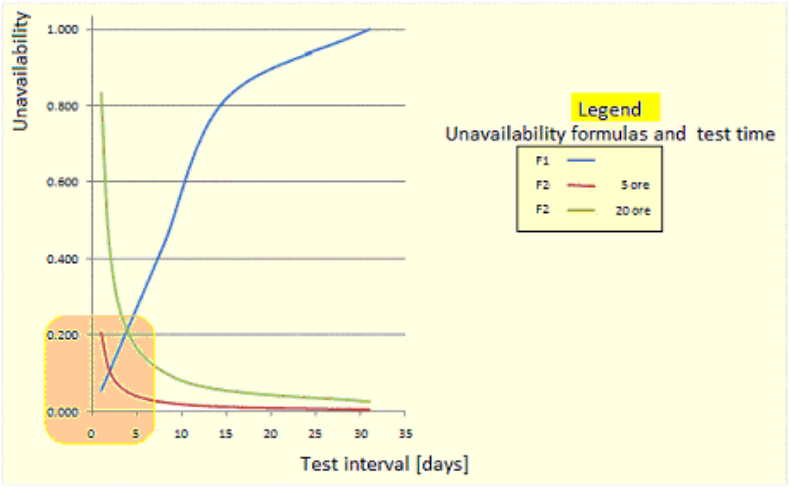

Fig. 7. Determination of the testing parameters for the analysed hydraulic circuit that use F1 and F3 formulas

In the table 7 are indicated the values obtained by solving the fault tree as a model of the two parallel HCs, by taking into account the testable component TK1 for which are applied the F1, F3 formulas to determine the optimum testing.

In the figure 7 are represented the curves that give the failure probabilities variation (by using F1 formula) with the test interval an test duration (F3). It is observed the close region of the curves for F1 and F3 formulas with the test durations of 5 respectively of 20 hours and the test interval between 1 – 31 days. This is a typical analysis specific to determine the test interval.

5. Conclusions

PSA studies in order to be credible must have developed specific models and as much as possible specific reliability data and parameters. Also the as possible the uncertainties in modelling and data allocation have to be minimized.

The paper presents an analytical (*probabilistic*) method and a calculation example that permit risk evaluation or nuclear facilities and intents to solve the data collection issues by adopting appropriate analyzing techniques like online data acquisition risk monitors developed based on intelligent and smart sensors.

The original data acquisition, transfer and processing method for risk monitors development, presented in this paper, prevents the situations where specific data and information are not included in the appropriate databases or processed for future analyzing and use.

The specific monitoring of risk, safety, reliability and processing based on intelligent and smart sensors and online and direct data acquisition, offers the following major advantages:

- *The event is recorded and processed immediately after occurrence;*
- *The components or equipment behaviour could be estimated and appreciations about the technological processes and life time trends could be performed;*
- *Decrease costs of data acquisition and SSC modelling or analyzing activities;*
- *Assist the facility operators and managers in taking decision;*
- *Different sensitivity analyses could be performed, also ageing estimation of SSCs and evolution of risk with time;*
- *The overall process of risk monitoring and facility modelling could be automated.*

The paper presents also a case study for the determination of a test interval for a hydraulic circuit. The method is based on specific PSA analysis activities, information, algorithms, criteria and relations, according to the fault tree and event tree modelling and additional analysis techniques, in order to obtain specific results for SSC model analysis.

By integrating the direct acquisition of data, the on-line risk monitor becomes specific to a studied facility or system and close to a hardware equipment rather than analytic instrument.

REFERENCES

[1] *G. Florescu, V. Panaitescu* et al, "A New Technique for Risk Monitoring based on On-Line Data Acquisition", Paper **S3-6** presented in Proceedings to SIEN 2007 conference, Bucharest;

[2] *G. Florescu*, *V. Panaitescu* et al, "Monitorizarea în timp real a riscului unei instalații nucleare" (Real time monitoring of risk in a nuclear installation), RAAN – SCN Pitesti, **Internal Report**, **2008**.

[3] *Ali Mosleh, A. Dias, G. Eghbali, K. Fazen,* An Integrated Framework for Identification, Classification, and Assessment of Aviation Systems Hazards, Proceedings to PSAM 5 conference, Berlin, 2004, **Paper 0676**.

[4] *Corwin L. Atwood, Robert W. Youngblood*, Application of Mixture Priors to Assessment of Performance, Proceedings to PSAM 5 conference, 2004, Berlin, **Paper 0034**.