AN APPROACH FOR ASSESSING RISK OF COMMON CAUSE FAILURES IN CRITICAL INFRASTRUCTURES

Eugene BREZHNEV

Abstract: This paper presents the technique for the critical infrastructure (CI) risk assessment based on Failure Modes, Effects and Criticality Analysis (FMECA), modified for multiple failures' criticality assessment. The multiple failures (MFs) are significant contributors to risk in critical infrastructure. In spite of the low frequency of multiple failures' occurrence, the severity of their consequences could lead directly to the CI's accident and malfunctions. The influences of multiple failures should be taken into consideration as early as possible at the design stage. The paper presents classification of MFs, their root causes and coupling factors that stipulate the common susceptibility of systems to shared cause. The common cause failures (CCFs) are a subset of the dependant multiple failures. The qualitative procedure developed in the paper considers the consequences' severity of CCFs on different I&C system levels. The total severity of CCFs is presented as a sum of severities for each level. The results of FMECA for single independent failures are taken as initial data to perform FMECA for MFs.

Keywords: Critical infrastructure, multiple failures, coupling factors, common cause failures, safety.

Introduction

The importance of critical infrastructure's (CI) safety provision is conditioned by the high consequence's severity of accidents and incidents during CI's operation. Thus nuclear power plant's (NPP) severity accidents are accompanied with radiation release into the atmosphere followed by environment contamination and increase of risk for people's health and lives.[1] The multiple failures (MFs) are of the main risk-factors which stipulate NPP risk accidents increase. The Three Mile Accident happened when three auxiliary pumps activated automatically failed while being called on demand. The multiple failures were caused by a violation of a key Nuclear Regulation Committee (NRC) rule, the valves had been closed for routine maintenance and the system was unable to pump any water. The same equipment's multiple failures

INFORMATION & SECURITY. An International Journal, Vol.28, No. 2, 2012, 199-210.

caused the Boston Edison's Pilgrim NPP's trip (April 1986) and Unit 1 of Nine Mile Point's trip (1987) etc.

The Instrumentation and Control (I&C) systems play a crucial role in the operation of NPP. The main objective of I&C systems in NPP is to ensure safety, availability and performance of the plant. The nuclear safety means the achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection public and environment from undue radiation hazards.

The NPP I&C's failures data analysis proves that MFs are significant contributors to the I&C incidents. Thus, 450 failures (out of 3000) fall on multiple failures during 564 reactor-years. The multiple failures cause the diesel-generator's trip, the malfunctions of the reactor trip breakers, the motor-operated valves, pumps, etc.

The MFs of the I&C combined with operator's errors could cause the significant accident in the nuclear power generating industry, resulting in the release of radioactive gases. The Chernobyl disaster is the most convincing example. The catastrophic accident was caused by gross violations of operating rules and regulations. During preparation and testing of the turbine generator under run-down conditions using the auxiliary load, personnel disconnected a series of technical protection systems and breached the most important operational safety provisions for conducting a technical exercise. A problem in the cooling system at Nine Mile Point 2 in New York, USA kept the nuclear plant from reopening on schedule. The plant had shut down because of a malfunctioning electronic system which occurred when a condenser valve was mistakenly closed during maintenance work being done on the plant's electrical system.

Defence-in-depth is employed to compensate for failures in other systems or functions. In practice, several independent systems are implemented to serve as successive barriers to prevent unsafe consequences from occurring. This aspect of the mitigation approach is especially effective against single failures. However, MFs can potentially disable the multiple barriers and result in unsafe conditions. MFs affect the multiple redundancies or systems within or among echelons of defence and constitute the principal credible threat to defeating the defence-in-depth provisions within the I&C system architecture of an NPP. MFs reduce the efficacy of one of basic NPP safety criterions – the single failure criterion (SFC). The criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure. The SFC, as a design and analysis tool, has the direct objective of promoting reliability trough the enforced provision of redundancy. The objective of SFC is to search for design weaknesses which could be overcome by increased redundancy. MFs decrease the safety integrity level by affecting the redundant systems.

Common cause failures (CCFs)

The NPP's operational experience proves CCFs are a subset of multiple failures and main contributors to the accident risk's increase. The CCFs are an important class of dependant events with respect to their contribution to the I&C unavailability. This is important for redundant or diverse systems. The failure of multiple components due to a common cause represents one of the most important issues in evaluation of the I&C reliability or unavailability.

The NPP's I&C failure statistics demonstrates that CCF contributes up to 29% of total amount of dependant failures. The CCFs are difficult to quantify correctly, i.e. it is difficult to know if a component fails due to a common root cause that affects several components, or if it fails because it is old and worn out.

There are many definitions describing CCFs. There are not correct definitions; the best definition depends on the field of use.[2] The authors proposed their own definition of CCF. They classified CCFs as the inability of multiple, first-in-line items to perform as required in defined time period due to single underlying defect or physical phenomena such that end effect is judged to be a loss of one ore more systems.

As an alternative definition, CCFs are defined as dependant failures in which two or more components' fault states exist simultaneously, or within short time interval, and are a direct result of a shared cause.[3] Yet another definition is given by the standard IEC 61511. The CCF is a failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channels system, leading to system failure.

To summarize, CCFs are characterized by the following features:

1. Two or more similar components have failed or are degraded. The failures occurred on demand, during testing.
2. The failures share a single cause and are linked by a coupling factor. The condition or mechanism through which failures of multiple components are coupled is termed as the coupling factor. The coupling factor is a characteristic of a group of components that identifies them as susceptible to the same causal mechanism of failures.
3. The equipment failures are not caused by the failure of equipment outside the established component boundary. These failures are dependant but are not CCF events.
4. The conditions which cause CCF have to affect multiple components simultaneously. Simultaneity, in this context, refers to failures that occur close enough in time to lead to the inability of multiple components to perform their intended function.

Classification of coupling factors which stipulate CCFs in I&C of NPP

As described earlier, for failures to originate from the same cause and be classified as a CCF, the conditions for the trigger or conditioning events have to affect multiple components simultaneously. Simultaneity, in this context refers to failures that occur close enough in time to lead to the inability of multiple components to perform their intended safety function for a PRA mission. As mentioned the condition or mechanism through which failures of multiple components are coupled is termed the coupling factor. I&C systems are affected by the set of coupling factors during all life cycle. The factors' impacts can't be avoided because of factors' permanency. They are inherent part of evolutionary progress of any complex system. The only approach here is to control them in purpose to reduce their influence on the I&C. The multiple failures' risk is right along. So we need to develop and implement the strategies of failure management to make the I&C system capable to provide the services, though possibly alternated or degraded in the face of various type of failures and disruption.

CCCG arrangement

The data's analysis related to the hardware and software, procedures, design of I&C system is performed for each its hierarchy's level. The Common Cause Component Groups characterized by common susceptibility for one root-cause are taken as result of this analysis. The Common Cause Component Group (CCCG) is a group of usually similar components that are considered to have a high potential of failing due to same cause. The CCCG arrangement as the result of components features' commonality analysis is shown in Figure 1.

CCF Root causes classification

There are a set of root causes that must be considered:

- Design/ manufacture/ construction /Maintenance inadequacy;
- Human actions (errors, omission);
- Procedure inadequacy;
- Environmental stress;
- Influences of internal environment of a component.

All of these events affect the CCCG and cause CCF.

For any I&C system could be introduced a complex parameter which characterizes its generic commonality (K_{GC}). This parameter considers its components similarity in the

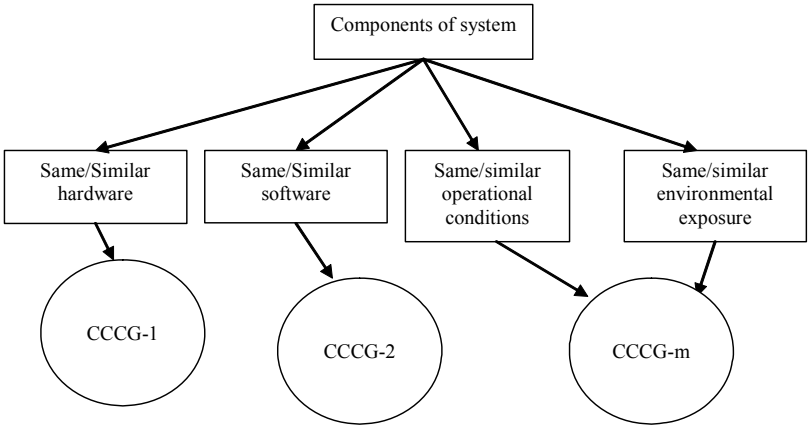

Figure 1: CCCG's arrangement (example).

space of the local coupling parameters (k_1, k_2, k_3, …, k_n). The local parameters proposed might be similarity of the equipment, procedures and location. The similar components are usually affected by the common design and manufacturing processes. The generic commonality might be assessed for each hierarchy's level of I&C system, for CCCG alone and between different CCCGs. The more value of generic commonality the more risk of CCF occurrence. This task might be resolved on the base of fuzzy clustering approach. The three-dimension interpretation of I&C generic commonality is shown in Figure 2.

CCF qualitative analysis methods

During the I&C design stage the qualitative analysis of measures' efficacy and sufficiency for providing reliability is performed. It allows determining the CCFs' root-causes and their consequences. There are some qualitative methods for CCFs analysis. Among them is:

- F*ault Tree Analysis*.[4] The fault tree analysis is a well arranged method of modelling the failure of a certain (top) event. The failure of a top event depends on other basic (physical) components. The dependencies between the components are modelled in a tree structure using AND- or OR-gates. As an example, consider a system of two - components, A and B. A fault tree with an AND-gate is used in the case where the top event (system) fails if both component A and B fail. This is similar to the parallel structure in a reliability block diagram. The OR-gate describes the event that the system fails if either component A or B fails. This corresponds to the series structure in a reliability block diagram. There are also other possible gates when dealing with fault trees, but these are not included in the present report. During

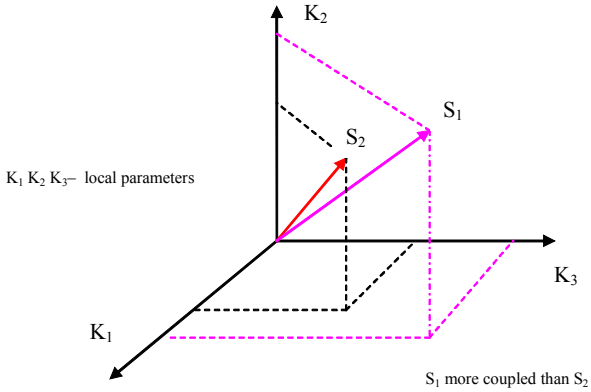

Figure 2: The three-dimensional space of I&C commonality for CCF analysis.

the constructing of fault tree a set of failures which could lead to system failure is complemented by CCFs. The FTA importance is based on ability to perform the analysis of possible failure's causes and give graphical representation for the following quantitative analysis of CCFs.

- *Event Tree Analysis* [5] is an inductive procedure that shows all possible outcomes resulting from an accidental (initiating) event (root-causes for CCFs), taking into account whether the installed safety barriers are functioning or not, and additional events and factors. By studying all relevant accidental events, the ETA can be used to identify all potential scenarios and sequences in the I&C system. Design and procedural weakness can be identified, and probabilities of the various outcomes from an accidental event can be determined.

FMECA application for CCFs criticality analysis in the I&C systems

The traditional FMECA [6] is an efficient technique to determine the potential failures' priorities and implement the qualitative assessment of their influences on I&C's safety. It is widely accepted that FMECA is not suitable for CCFs analysis and considered to be one of its disadvantages. One of stage of PSA procedures for CCF is a qualitative analysis performed to decrease the amount of calculations of quantitative stage of PSA. The aspiration is to avoid the calculations difficulties and increase the results' credibility by the improvement and adaptation of the single failure's analysis methods (SF FMECA) for multiple failures' criticality assessment. In the paper the complement of FMECA-based approach for MFs' qualitative criticality assessment in the I&C is suggested.

It is worth to note the further FMECA improvement for MF's assessment shouldn't lead to complication of the procedure for criticality's qualitative assessment considering the computation difficulties. The FMECA disadvantages should be taken into

account too. The approach proposed in the paper takes into consideration the principle of mutual failures' influences. The failure of one system might lead to changes of criticality of another system. The criticality is changed not only because of the failure frequency changes, but the severity of possible losses' changes.

FMECA approach for CCF's criticality analysis suggests taking into consideration the principle of hierarchy. Complying with this principle I&C system consists of hardware and software of different levels. The hardware is represented by the hierarchy of elements, functional units and blocks. CCFs on elements' level result in failures on functional unit's level. CCFs on functional unit's level cause blocks' failures, which in their turn lead to system's failures as whole.

Stages of CCF criticality assessment of FMECA-based approach

The CCF scenarios determination

The CCF scenario is a combination of root cause and CCCG considered being sensitive to it. The determination of root-causes is based on operational experience for specific I&C. In this case the part of CCCG and roots are eliminated from analysis and determined to be not significant contributor to I&C system unavailability. The result of this stage is a set of root-causes (RC) for the I&C given and a set of CCCG characterized by susceptibility to the root-causes mentioned:

$$CCF = \{CCF_1, CCF_2, CCF_i, CCF_m\} = \{(RC\text{-}1, CCCG\ 1, CCCG\ 2), (RC\ 2, CCCG\ 3)\ (RC\ 3, CCCG\ 4), (RC4, RC\ 5, CCCG\ 5), (RC\ m, CCCG\ l)\},\ m = \overline{1,M}, l = \overline{1,L}. \quad (1)$$

The qualitative screening of CCCG

Screening is a type of analysis aimed at eliminating factors that are less significant for protection or safety, in order to concentrate on the more significant factors. Screening is usually conducted at an early stage in order to narrow the range of factors needing detailed consideration in an analysis or assessment. The priorities of CCCG are determined considering the results of FMECA for single failures (SFs). The total value (taken as a sum) of criticalities for SFs related to one CCCG is a priority for this CCCG. All CCCGs' priorities are put into order. As shown in Figure 3 the maximal priority would be referred to CCCG with most components over criticality diagonal of FMECA table. The least is referred to CCCG with the most components are under criticality diagonal of table. The medium priority value is for CCCG with the components distributed not only under criticality diagonal of FMECA table, but over it.

Qualitative screening CCFs' basic events in CCCG. Classification of common cause basic events

The common cause basic event (CCBE) is an event involving common cause failure of a specific subset of components within a common cause component group. Let's

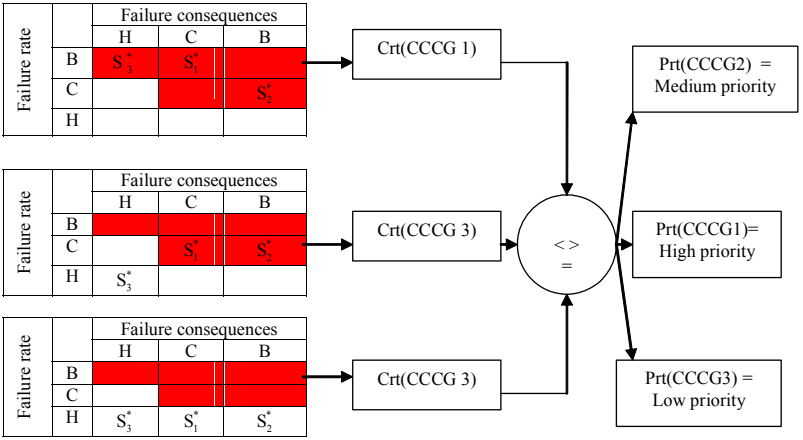

Figure 3: Qualitative screening CCCGs' priority based on results SF FMECA.

consider a system which consists of three subsystems. Then among three independent failures S_1^*, S_2^*, S_3^* caused by independent reasons we have some combinations of CCF determined as CCBEs, S_{12}^*, S_{13}^*, S_{23}^*, S_{123}^*, where S_{12}^* stand for CCF of two systems (1,2), S_{123}^* is stand for CCF of three systems (1, 2, 3). The CCBEs are put into order considering their priorities taken as results of SF's criticalities summation.

The result of this stage is elimination of CCBEs considered being not significant contributors to the risks for safety system.

Determination of CCF rate

For each CCBE could be evaluated its rate according to certain qualitative scale. For PSA there are three data sources used to select equipment failure reports to be reviewed for CCF events identification: (1) the Nuclear Plant Reliability Data Systems (NPRDS), which contains components failure information from 1980 through 1996; (2) the Equipment Performance and Information Exchange (EPIX), which contains components failure information since 1997; (3) LER Search, which contains Licensee Events Reports (LERs). All events that meet the CCF criteria are identified as CCF events and are included in the CCF database. The database contains CCFs beginning in 1980 and is continuously updated to remain current. The following failure rate's categories for each CCBE criticality assessment might be used presented in Table 1.

The CCF severity determination

The severities of CCFs are characterized by the system's resource decreasing. The system assigns certain amount of resource to compensate the losses of system's performance. It's suggested to represent the failure's consequences as a hierarchy of dif-

Table 1. Frequency rate categories for CCBEs.

Categories	*Qualitative descriptions*	*Quantitative descriptions (per year)*
A	Frequent	Once per month or more often
B	Probable	Once per year
C	Occasional	Once per 10 years
D	Very Remote	Once per 100 years
E	Very unlikely	Once per 1000 years or more seldom

ferent levels. The failure's consequences are considered for different I&C levels. The elements' failures consequences affect the I&C on all its levels, beginning from the functional units and propagating up through upper levels – blocks, subsystem and finally influence the system performance as a whole. The total CCFs' consequences severity is the integral function of consequences severity for all hierarchical levels of I&C considered. The priorities of consequences severity for different system's levels might differ. There are several approaches to determine the total consequences severity for CCFs. As the FMECA for multiple failures is a qualitative method then the total severity consequences could be evaluated as a sum of quantitative ranks related to the severity categories. Also the linguistic approach might be used for this purpose based on the computing with words (CWW) procedures.

There are values of CCFs' severity consequences for different system's levels shown in the Table 2.

CCBE – one of possible combination of elements' failures of one functional unit (for CCCG which comprises the FU's elements). There is a hierarchy of criticality ma trixes made for CCF shown in Figure 4. Three channels system S_{01} is a part of SoS.

Table 2. The values of CCFs' severity consequences for different system's levels. $CCBE_i$ belongs to CCCG.

	Consequences for functional unit			Consequences for Functional block			Consequences for Subsystem			Consequences for System		
	L_1	M_2	H_3	L_1	M_2	H_3	L_1	M_2	H_3	L_1	M_2	H_3
$CBEE_1$		×		×			×				×	
$CCBE_2$	×			×			×				×	
…..	……..											
$CCBE_m$			×			×			×			×

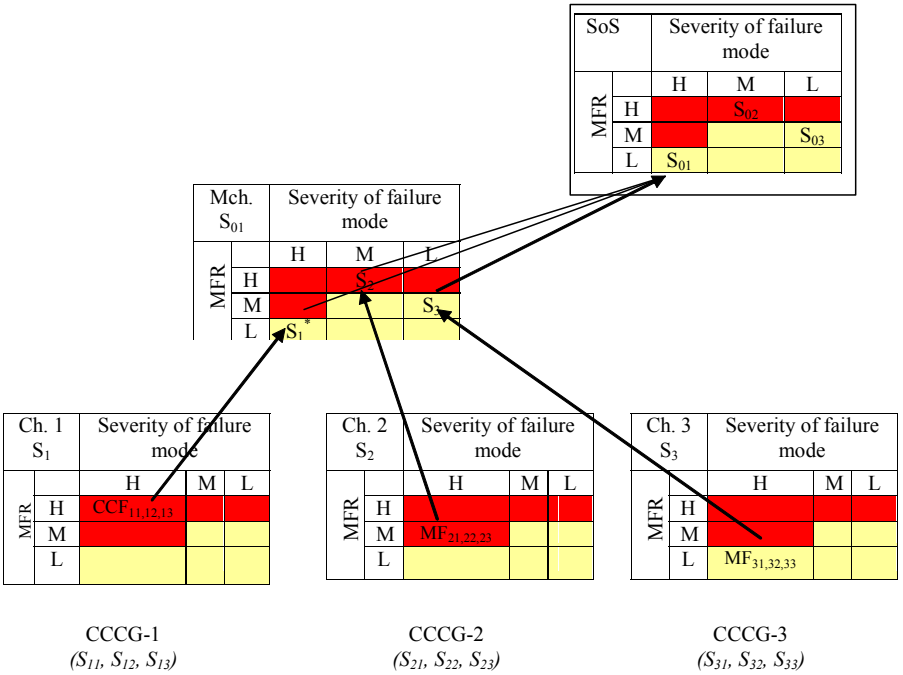

Figure 4: The hierarchy of criticality matrixes made for CCFs.

Thus as an example, the CCFs of elements S_{11}, S_{12}, S_{13} of the first channel leads to the S_1^* failure and change of criticality and degradation of S_{01}. The degradation of S_{01} leads to performance's change of SoS.

CCFs' criticality assessment

The results of this stage are CCFs' criticalities values inside of each CCCG. For each CCBE in CCCG the criticality value is determined as:

$$Crt(CCBE^{i}_{CCCG}) = S^{CCBE_i} * Fr^{CCBE_i}, \quad (2)$$

where $Crt(CCBE^{i}_{CCCG})$ - *CCBE's* criticality in CCCG; S^{CCBE_i} - *CCBE's* consequences severity $(CCBE_i \in CCCG)$; Fr^{CCBE_i} - frequency of $CCBE_i \in CCCG$.

The post Three Mile Island accident analysis based on MF FMECA

Let's consider the MF FMECA application for Three Mile Island (TMI) accident's analysis. The most serious nuclear reactor accident to date in the United States occurred at 4 A.M. on March 28, 1979, at the Three Mile Island nuclear power plant outside Middletown, Pennsylvania. Operator errors in dealing with the feeding pumps

that had shut down caused the Unit 2 pressurized-water reactor to lose coolant and overheat. The error was made during the maintenance procedure. Three valves were closed. This is an example of CCFs caused by the human error. The emergency water feeding system (EWFS) consists of thee pumps: S_1, S_2, S_3 (see Figure 5).

The set of EWFS's states is determined by: independent failure of S_1^* S_2^*, S_3^*; $CCBE_1$ - CCFs of the first and second pumps S_{12}^*; $CCBE_2$ - CCFs of the first and third pumps S_{13}^*; $CCBE_3$ - CCFs of the second and third pumps S_{23}^*; $CCBE_4$ - CCFs of all pumps S_{123}^*. The independent pumps' failures were analyzed during the TMI design stage. The FMECA for independent single failures of emergency water feeding system was performed during design stage. The FMECA table might have represented as shown in the table 3. It contains the SFs' criticalities.

Thus CCFs of pumps were not considered. MF FMECA implies considering the simultaneous failures of two and more pumps. The FMECA table for pumps' CCFs is shown in Table 4. If FMECA team had performed FMECA for MF at design stage, the Three Mile accident might have been avoided.

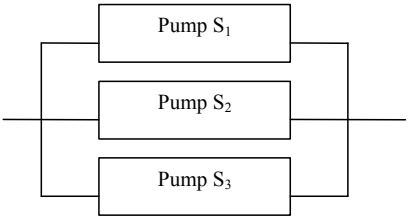

Figure 5: The emergency water feeding system (general).

Table 3. The FMECA table for SF.

		Severity of CCF		
MFR		H	M	L
	H		S_2	
	M		S_3	
	L	S_1		

Table 4. The FMECA table pumps' CCFs

		Severity of CCF		
MFR		H	M	L
	H			
	M		S_{13}^*, S_{23}^*	
	L	S_{123}^*	S_{12}^*	

As it is seen from MF FMECA table CCFs of three pumps is indeed very seldom event. But severity could result to risk accident increase as it really happened. The consideration of pumps' CCFs might have provided the basis for risk assessment to determine what the potential consequences are associated with CCFs of pumps, identify techniques to manage the risk or mitigate its consequences.

Conclusions

The need of decrease the risk of the multiple failures' occurrence in the I&C system stipulate the development of available techniques of the SF's qualitative analysis and their adaptation for MF's criticality analysis. The improvement for MF FMECA is based on the SF FMECA. The qualitative analysis performed at the design stage of I&C system allows reducing the laboriousness of PSA's stages performed during CCF analysis. Proposed approach may be applied to safety analysis of NPP I&C as a set of complex systems. Next step of technique enhancement will be related to consideration the cascading failures occurred in critical infrastructures.

Notes:

[1] *Risk Management: A Tool for Improving Nuclear Power Plant Performance*, IAEA-TECDOC-1209 (Vienna: IAEA, 2001).

[2] A. Mosleh, et al., *Guidelines in Modeling Common Cause Failure in Probabilistic Risk Assessment*, NUREG/CR-5485 (November 1998).

[3] A. Mosleh, et al., *Procedures for treating Common Cause Failures in Safety and Reliability Studies. Analytical Background and Techniques*, NUREG/CR-4780 ERPI NP-5613, Vol. 2 (2000).

[4] Gerhard Schellhorn, Andreas Thums, and Wolfgang Reif, "Formal Fault Tree Semantics," paper presented at the Sixth World Conference on *Integrated Design & Process Technology*, Pasadena, CA, 2002.

[5] Marvin Rausand, "Event Tree Analysis," in Marvin Rausand and Arnljot Høyland, *System Reliability Theory: Models, Statistical Methods and Applications*, Second edition (Hoboken, NJ: Wiley, 2004), 108-117.

[6] J.B. Bowles, "An assessment of PRN prioritization in a failure modes effects and criticality analysis," *Journal of the IEST* 47 (2004): 51-6.

EUGENE BREZHNEV – see CV on p. 78 of this volume.