Application of dynamic system reliability methods for incorporation of age-dependent reliability parameters and data into the PSA model

Gueorgui Petkov

Second International Symposium on Nuclear Power Plant Life Management

Shanghai, China
October 15 – 18 2007
Resume

- System, Structure and Component (SSC) failures and repairs are implemented in time and consequently they are age-dependent.

- The paper presents the two alternative dynamic system reliability approaches - GO-FLOW and ATRD (Analysis of Topological Reliability of Digraphs) - to extend the FT (Fault Tree) methodology for NPP aging systems.

- Alternative methodologies are used to investigate the feasibility of increasing of failure, restore and repair rates of all component categories to take into account aging process in NPP availability.

- Both approaches are used for preparation of comparable aging process component and system models of a WWER-1000/V320.
Introduction

- Approaching the end-of-design-life and safety margins, the lifetime management becomes not only an immediate technical task but an essential political, economical and social requirement.
- This problem nowadays is one of the greatest concerns of engineers and scientists of industry and also a topic of national and international discussions.
- These discussions give a new meaning to economical and political reality.
- The questions of free competitiveness, rights and obligations following social and environmental risk of NPP have been brought out.
The first four units of Bulgarian Kozloduy NPP with reactors WWER-440/V230 have been already decommissioned because of external political reasons and economical factors.

The ‘old’ units’ safety and aging problems were of primary importance for modernization and reconstruction measures implementation. These measures were not sufficient to convince the public opinion and some our partners to perceive the risk from these NPP units without prejudices!

Both the modernized NPP and the new one should be operated for extended period of time and efficient Plant Lifetime Management (PLiM) is a very important issue. It includes:

- an investigation of the impact of aging effects on NPP safety,
- justification, spreading and popularization of NPP risk-reduction measures.
Incorporation of age-dependence

- The aging process could take place as gradual degradation or improvement of characteristics of materials.
- Aging can affect systems and structures only through their components. The APSA (fault trees’) models are modified on the level of component basic events only.
- The preferable way to take into account the SSC susceptible to aging is to embed external physics-based reliability models directly into the PSA software and to update the component reliability database of already calculated models - hybrid deterministic-probabilistic models.
- The “plug-in” concept allows easy integration of external calculation and extension by alternative dynamic SSC/processes models.
IAEA-CN-155/031

Age-dependent reliability description

Unrepairable components

\[ \lambda(t) = \lambda_0 + \alpha(t)(t - \tau) \quad (1) \]

\[ \lambda(t) = \lambda_0 + \alpha(\beta + 1)(t - \tau)^\beta \quad (2) \]

Repairable components

\[ \lambda(t) = \lambda_0 + \alpha(t)(t - t' - \tau) \quad (3) \]

\[ \lambda(t) = \lambda_0 + \alpha(\beta + 1)(t - t' - \tau)^\beta \quad (4) \]

\[ \lambda_i = \lambda_0 / \gamma^{i-1}(t) \quad (5) \]

- \( t \) - the global time,
- \( \lambda_0 \) - pre-aging constant failure rate,
- \( \tau \) - the threshold time at which aging starts and
- \( a(t) \) - rate of degradation process
- \( \alpha \) - scale parameter
- \( \beta \) - shape parameter
- \( \tau \) - location parameter
- \( t' \) – the local time at which last repair/restore was completed
- \( \gamma(t) \) - degradation factor (0<\( \gamma \)<1)
Reduction of risk and unavailability

The plant availability and safety may decrease due to the aging of unrepairable and repairable components.

The resulting increase could be reduced by different maintenance measures:

- replacements and upgrading of renewable (repairable and restorable) components during repairs
- changing of surveillance intervals of renewable components
- setting the trend of the degradation factor to unit.
Categories of ageing components

- **Category 1. Unrepairable or irreplaceable components**
  - unrepairable (non-restorable) irreplaceable components (Fig.6),
  - restorable irreplaceable components (Fig.5).

- **Category 2. Repairable hard-to-replace components**
  - non-restorable hard-to-replace components (Fig.4),
  - restorable hard-to-replace components (Fig.3).

- **Category 3. Replaceable on a routine basis components**
  - non-restorable replaceable components (Fig.2),
  - restorable replaceable components (Fig.1).
State transition diagram of gradually aging component with multiple failure modes.

- Aging State 1 (New) → Component Restored: $\mu_1$
- Aging State 1 → Component Degrades: $\lambda_1$
- Aging State 2 → Component Fails: $\lambda_2$
- Aging State 2 → Component is Repaired: $\mu_2$
- Aging State n → Component Fails: $\lambda_n$
- Aging State n → Component is Repaired: $\mu_n$
- Failure Mode 1 → All Failure Modes: $\lambda_{21}$
- Failure Mode 2 → All Failure Modes: $\lambda_{22}$
- Failure Mode m → All Failure Modes: $\lambda_{2m}$

Transition rates are denoted by $\lambda$ for failure rates and $\mu$ for repair rates.
Fig. 1. Restorable replaceable component

- Aging State 1 Continues
- Aging State 1 (New)
- Component Restored
- Component Degrades
- Failure Mode 1 Continues
- Failure Mode 1
- Failure Mode 2 Continues
- Failure Mode 2

- Aging State 2 Continues
- Aging State 2
- Component Fails
- Component is Repaired
- Failure Mode 2
- Failure Mode m Continues

- Aging State n Continues
- Aging State n

- Replacement
- λ₁
- µ₁
- λ₂
- µ₂
- λₙ⁻¹
- µₙ⁻¹
- λₙ
- µₙ

- All Failure Modes
- λ₂₁
- µ₂₁
- λ₂₂
- µ₂₂
- λ₂m
- µ₂m

- All Failure Modes
Fig. 2. Non-restorable replaceable component

- Normal State
- Failure Mode 1
- Failure Mode 2
- Failure Mode m

- Replacement
- Component Fails
- Component is Repaired
- All Failure Modes

- λ_{21}
- μ_{21}
- λ_{22}
- μ_{22}
- λ_{2m}
- μ_{2m}

IAEA-CN-155/031
Fig. 3. Restorable hard-to-replace component

IAEA-CN-155/031
Fig. 4. Non-restorable hard-to-replace component

- Normal State Continues
- Component Failed
- Failure State Continues
- Component is Replacing

\[ \lambda \]
Fig. 5. Restorable irreplaceable component

1. Ageing State 1 Continues
   - $\mu_1$: Component Restored
   - $\lambda_1$: Component Degrades

2. Ageing State 2 Continues
   - $\mu_2$
   - $\lambda_2$

3. Ageing State $n$ Continues
   - $\mu_{n-1}$
   - $\lambda_{n-1}$

- Ageing State 1 (New)
Fig. 6. Unrepairable irreplaceable component
Definition and quantification of states & modes’ transition diagrams of aging components

\[ \Lambda = \begin{pmatrix} \lambda_{11}, \lambda_{12}, \ldots, \lambda_{1m} \\ \lambda_{21}, \lambda_{22}, \ldots, \lambda_{2m} \\ \vdots \\ \lambda_{n1}, \lambda_{n2}, \ldots, \lambda_{nm} \end{pmatrix} \quad \text{and} \quad \mu = \begin{pmatrix} \mu_{11}, \mu_{12}, \ldots, \mu_{1m} \\ \mu_{21}, \mu_{22}, \ldots, \mu_{2m} \\ \vdots \\ \mu_{n1}, \mu_{n2}, \ldots, \mu_{nm} \end{pmatrix} \]

where \( i=1 \ldots n \) - numbers of possible aging states;

and \( j=1 \ldots m \) - numbers of possible failure modes.
Simplifications of the APSA models

For renewable component Availability is

\[ A(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t} \]  

(7)

and Unavailability is

\[ Q(t) = 1 - A(t) = \frac{\lambda}{\lambda + \mu} \left[ 1 - e^{-(\lambda + \mu)t} \right] \]  

(8)

for unrepairable component Reliability is

\[ R(t) = A(t) = \exp(-\lambda t) \]  

(9)

and Unreliability is

\[ F(t) = Q(t) = 1 - \exp(-\lambda t) \]  

(10)
Pseudo-constant rates assumptions

1. The component is in its prime of life;
2. the given component is large with many sub-components having different rates or ages;
3. the data are so limited that elaborate mathematical treatments are unjustified.

The above matrices and vectors could be simplified for each sub-category of components by:

- equations (1)÷(5),
- age discretization,
- flexible formulation of boundary conditions.
1) Why could be dynamic system reliability methods useful extensions to the APSA model?

- The conventional ET-FT methodology for reliability and risk assessment is designed to describe static relationships between logical variables and does not explicitly treat time, physical process variables, aging or human behavior.
- The overcoming of quasi-static tree models limitations needs essential extensions or alternative methodologies for due assessment of reliability and risk.
- Dynamic aspects of hardware-software-liveware systems and processes require more advanced tools to analyse them.
- The alternative methodologies should include extensions of the ET-FT approach, rather than revising the methodology itself.
- However, alternative methods could be intended also to supplant the ET-FT approach in certain situations.
2) Why could be dynamic system reliability methods useful extensions to the APSA model?

- It is possible to reduce the component multiple state model to the approximative two-state model that is quite applicable for the FT technique and no other modifications are necessary.

- If the approximation errors of these calculations are not negligible then the Markov transition diagrams must be constructed and solved (Figures above). However:
  - the conditional intensities are age-varying unknowns
  - it is quite complicated to solve analytically the model with many dependent and compatible aging states and failure modes.

- Such alternative methods may give more
  - flexibility
  - convenience
  - applicability for incorporation of age-dependent effects and dynamics of physical processes.
An important characteristic of natural and engineering systems and processes are that they behave dynamically.

System and process dynamics evolves over time:

- System components interaction with each other and with environment.
- System components response to initial perturbations and changes of process variables.
- System configuration changes depending on the required mission or occurrence of component failures.
- Components’ characteristics depend on their condition, standby or operating.
Alternative methods applicability

The applicability of one or another alternative methodology for dynamic system reliability modeling depends on:

- analysis level
- quality of database
- available knowledge of structural (physical and logical) and functional system relationships
- possibility to compare, validate and verify the methodology results.
Spectrum of methodologies

- **ET/FT extensions**
  - Expanded ETs
  - GO-FLOW
  - Digraph-based FT construction

- **Explicit state-transition methodologies**
  - Event sequence diagrams (ESDs)
  - Explicit Markov chain models (controlled by global clock)

- **Implicit state-transition methodologies**
  - Continuous ETs (semi-Markov chains – local clocks are added to the global clock)
  - DYLAM
  - Dynamic ETs (DETAM)
  - Discrete event (Monte Carlo) simulation

- **State-merging technique or “cell-to-cell” approach**
  - Analysis of Topological Reliability Digraphs
GO-FLOW Methodology

- It is a success-oriented system reliability analysis methodology.
- GO-FLOW chart is constructed with standardized operators and signal lines.
- Analysis is performed by one GO-FLOW chart and one computer run.
- GO-FLOW analysis support system has been developed.
- Developed by Matsuoka & Kobayashi (National Maritime Research Institute, Japan, in 1988)
GO FLOW Procedure

Conceptual image of GO-FLOW analysis procedure.
Explicit Markov Chain Models

- Probabilistic system behavior is simulated by the Markov chains - a set of first order differential equations with feedback describing the interaction between system variables.
- Reliability space - failure and repair rates for components.
- Discrete state space – time representation of system dynamics.
- The action of operational control components are specified by the control laws and the system fails if any process variable is outside the control space.
- Developed by Tunk Aldemir (Ohio State University, USA, in 1987).
Explicit Markov Chain Procedure

1. Identifying the control regions
2. Choosing partitioning
3. Determining operational and failed states
4. Mechanized construction of transition matrix
DYLAM Methodology

- **Dynamic Logical Analysis Methodology**
- Combination of process simulation and probabilistic model
- DYLAM is a computer program
- Developed by Cacciabue & Cojazzi (EU JRC Ispra, in 1983)
Conceptual image of DYLAM analysis procedure.
ATRD Methodology

- The ATRD method uses inductive logic where every physical and logical connection should be expressed in an explicit form.
- The ATRD system model is a digraph of system functioning. Reliability networks are presented as stochastically independent or dependent graphs.
- The multiple network with control links (Petri Nets elements) or places can discretely, hierarchically and dynamically change the state of the system components.
ATRD spectrum of applications

- Risk and Reliability Modeling of Process Control Systems and Measurements
- Dynamic Modeling of Physical Phenomena (Fire Analysis)
- Phased Mission Analysis
- Data Estimation and Collection
- Analyzing Human Actions in PRA and Accidents
- Dynamic Decision-making and Management Analysis
- Risk and Reliability Modeling of Human-Machine Systems
- Dynamic System Diagnostics and Modeling
A ‘cell-to-cell’ ATRD procedure, called ‘matreshka’, is used to transform the complex dynamic system into a system of modules.

- Each module represents a 3-component dynamic system with 4 states (cube).
- The ATRD method traces each event sequence in cubes.
- Developed by G. Petkov (Moscow Power Engineering Institute, Russia, in 1992)
4-state dynamic system reliability model
Precautionary insights

AND 3-component system and OR 3-component system by 3 methods
Preliminary conclusions

- The addition of the time dimension leads unavoidably to a more complicated analysis.
- All methodologies are significantly more complex and have more extensive data requirements.
- The analyst needs to ensure that extra capabilities of the methodologies are indeed needed.
- The approaches allow an integrated treatment of aging process variables, hardware states and failure modes.
Intents of case study ‘Age-dependent safety system reliability model’

- To investigate the feasibility of dynamic system reliability methods, GO-FLOW and ATRD, for:
  - increasing of failure, restore and repair rates of all component categories or
  - reducing the surveillance intervals of repairable components to take into account aging processes in plant availability.
- To prepare comparable FT, GO-FLOW, ATRD aging process component and system models (3-train RHRS of WWER-1000/V320);
- The case study comprises three categories of aging components:
  - restorable replaceable (FIG.1) – valves, pumps;
  - non-restorable replaceable (FIG. 2) – check valves and pipes;
  - restorable hard-to-replace (FIG.3) – tanks and heat exchangers.
Insights (1)

- The dynamic system reliability methods could be used to allocate the aging reliability data for basic events and aging failure mode and effect analysis.
- The aging processes description of safety systems differs from the processes of normal operation systems and must include aging in working and stand-by states at different intervals.
- The proposed decomposition of aging states seems appropriate.
- The failure mode database is concerned with component functions and rarely with physical component processes, including aging related processes.
- It means that only part of component failure modes should be suspected of aging.
- The quantification of age-related degradation effects must be sensitive to component’s function.
Insights (2)

- The GO-FLOW and ATRD methods could be used for calculation and synchronization of the aging impact to the safety system component unavailabilities.
- They may extrapolate and predict the component unavailability curves up to stationary values, in different time intervals and to the end of plant lifetime.
- ATRD seems more appropriate for explicit obtaining of dynamic component unavailability functions and data preparation because the GO-FLOW results depend on calculation step and available operator type values.
- However, the GO-FLOW operators have been increasing.
- GO-FLOW could be especially useful for extrapolation of component/system unavailability curves in different time intervals.
Insights (3)

- All dynamic system reliability methods could be used to propose the optimal periodical test and preventive maintenance intervals for components based on determined options and criteria.
- A practicable approach seems to be the use of different individual aging process and component degradation and restoration factors.
- The shortening of surveillance intervals for renewable components, as an aging compensation measure, would be more explicitly modeled and treated in PSA if a restoration factor, similar to degradation factor, is introduced.
Continuation and extension of CS ‘Age-dependent safety system reliability model’

The case study will be continued and extended to:

- assess system interactions based on degradation mechanisms and component aging behavior
- identify the necessary FT modifications (additional gates, basic events, parameters and structure changes)
- perform sensitivity study with the GO-FLOW and ATRD methods.

Additionally, the impact of FT loop-free and Markov process’ ‘slow-fast’ approximations is to be evaluated.

A normal operation system aging case study should be conducted in parallel for better understanding how to incorporate aging effects into PSA applications.