European Safety and Reliability Association

Newsletter

http://www.esrahomepage.org June 2013

# Editorial

*Enrico Zio*
*ESRA Chairman*
*Politecnico di Milano, Italy*
*École Centrale Paris,*
*Supelec, France*

Dear ESRA member,

Summer has arrived and we are all getting ready for vacations! This period will allow us to recharge our batteries for our upcoming event: ESREL 2013 in Amsterdam.

The organization for ESREL 2013 is well in place, with approximately 400 papers to be presented, interesting keynote lectures by knowledgeable and esteemed colleagues, panel discussions and pleasant social activities. We will also have our General Assembly to share the situation of our Association and decide together on its future activities. By the way: make sure that you have regularized the payment of your membership to the Association, to support it and participate in it (if you have not yet regularized your membership position, please contact us and we will send you the necessary information and invoice).

As we are approaching ESREL 2013, we are already working on ESREL 2014 in Wroclaw and thinking of ESREL 2015: the call for proposals of venues has been launched and we are eagerly waiting for yours. Take the initiative!

During this period, ESRA has also been involved in, sponsored and participated to a number of activities with our members. Of these you will read in the Newsletter directly by our involved colleagues.

Finally, I look forward to join you in Amsterdam and wish you enjoyable summer vacations.

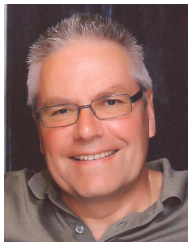
With kind regards,

Enrico Zio
Chairman of ESRA

# Feature Articles

## Risk Assessment of IT Systems: A Tentative Affair?

*Ralf Mock*
*Zurich University of*
*Applied Sciences ZHAW,*
*Switzerland*



*Hugo Straumann*
*Swisscom AG,*
*Switzerland*

Experts in risk assessment have built up a decade long knowledge base on how to analyse and manage complicated and complex technical systems. The area of successful application covers nuclear power

generation, aviation, automotive among others. This state of the art is also reflected by a bulk of standards about risk analysis, assessment and management in many industrial branches. However, its overall success story is definitely not repeated in Information Technology (IT). In this "opinion paper", the authors first outline, why risk assessment missed the bus in IT in the area of IT security. The second section shortly shows the current status of risk assessment at IT operating companies. Finally, a synthesis between compliance approaches and risk assessment is discussed.

Risk assessment and IT analysis approaches are historically the results of independent as well as time-displaced developments. In the late 1940s, the development of system analysis approaches mainly arises from military and mechanical engineering, followed by chemical (1960s) and nuclear engineering (1970s). The then introduced approaches (as FMEA, HAZOP, Fault Tree Analysis, Event Tree Analysis, as well as the PSA framework) are still core elements of risk assessment. Electronic engineers have started their IT system analysis activities without knowing (or by ignoring) these methodologies in the late 1970s. This staggered development generated, for instance, a mess in definitions of risk assessment terms. It was not until before 2000 to manage the harmonisation of standards. However, the IT experts still (and exclusively) use IT system analysis approaches of their own, as CRAMM [2], COBIT [3], OCTAVE [4], CORAS [5], among others. There is no mutual exchange of experience in risk assessment of complex systems (at least, this discussion has not found its way into enterprises or practical engineering). The risk assessment approaches are still tailored to the needs, customs, as well as operational and specific economic environments of their root industries, e.g. nuclear power generation. For instance, the temporal horizon to do a full scope PSA in nuclear power generation comprises years; a full scale risk analysis of, e.g., a big computing centre, has typically to be finished within three months (or less). Beyond all differences in technology and hazards, the allocated resources finally determine the (practical) applicability of any risk assessment approaches. Hence, Fault Tree Analysis or Markovian chains, etc. are virtually not found in IT.

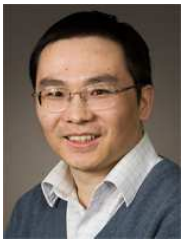
Although there have been some efforts about 10 years ago, risk analyses are currently not propagated in IT according to our experience. The risk approach is frowned down and is considered as waste of time and money. In the meantime, the focus has been shifted to compliance checks going along with a policy shift in IT security culture at enterprises. Those responsible for IT security now fully concentrate on policies and checklists regarding compliance. These activities have resulted in a well-developed basic protection of IT systems at enterprises. Looked at more closely, this trend reveals weaknesses with regard to risk management: The fixing on compliance (and associated policies) results in less flexible patterns of risk management or even in blind spots. For instance, BYOD (bring your own device) is a trend to consumerisate hardware and tools at enterprises. However, many IT security policies do not allow the mix up of private and business affairs by shared devices – and disregard it. However, this is far from reality as people use their devices in order to do their business in the most effective or comfortable way. BYOD cannot be stopped and IT security quickly becomes perceived as inflexible "business preventer". As compliance checks rely on known drawbacks (i.e. they reflect the state of technology), undesired events beyond standards will not be identified. This first undermines Defence-in-Depth principles and secondly pushes low probability high consequence risks out of the IT management's scope. As most enterprises (at least most SME) never experienced a severe business interruption by IT system failures (as exemplified in [1]), they consider it to be a residual risk which can be ignored. At best, worst cases and catastrophic scenarios are covered by Business Contingency/Recovery strategies (if and when). Likelihoods are regarded as not relevant. Even worse, over-regulation eats up the safety budgets at enterprises and there are no resources left to take measures against the unexpected.

In summary, in the authors' point of view, this is an unsatisfying situation in the IT field: Established risk assessment approaches are mostly not attractive to enterprises as they struggle to encompass the dynamic, fast modification rate of IT as well as business constraints. On the other hand, compliance checks are practical but quickly brake business and ignore the rare and uncommon. The way things are going, a synthesis is needed to bring back risk analysis to IT operating enterprises. As known from the authors' own experience, compliance checks are adequate to ensure a sufficient level of basic protection (in IT security) at normal system operation. However, compliance check activities should be restricted on this level. Regulation that is too restrictive and slowing down business will be sidestepped anyway. On the other hand, the risk assessment methodology is well tailored to deal with the exceptional, unplanned and unforeseen. For instance, it could support project developer to find the best (or adequate) solution with regard to IT security. With this, the IT security would shift from "preventer" to "enabler" and risk assessment would find the appropriate position within the management of enterprises. Applied R&D is challenged to provide practicable concepts and approaches, e.g., (generic) check lists and web-based tools for risk assessment purposes in close cooperation with industrial partners. There is a surprisingly open field in order to find "proper" risk assessment approaches which base on risk analysis theory, consider IT security issues and which are business-compatible.

[1] Mock, R., Stern, O., Knaack, R. and E. Kollmann (2012). Higher Education in Informatics – Concepts and Lessons Learnt (PSAM 11 & ESREL 12), Helsinki, Finland.

[2] CRAMM, Central Communication and Telecommunication Agency Risk Analysis and Management Method; www.cramm.com
[3] COBIT, Control Objectives for Information and Related Technology; www.isaca.org
[4] OCTAVE®, Operationally Critical Threat, Asset, and Vulnerability Evaluation℠; www.cert.org/octave/
[5] CORAS, A Platform for Risk Analysis of Security Critical Systems; www2.nr.no/coras/

# Fault Diagnosis using Support Vector Machine (SVM)



*Yuan Fuqing*
*Associate Lecturer*
*Division of Operation and Maintenance Engineering*
*Luleå University of Technology*

*Uday Kumar*
*Professor*
*Division of Operation and Maintenance Engineering*
*Luleå University of Technology*

Nowadays engineering system is turning to be more and more complex. The amounts of data collected from the system are huge and it is growing exponentially. Utilization of these data to diagnose the failure in its early stage will be useful for prevention of catastrophic failures. However, these data are interconnected from each other, and their inter-dependency among these data is possibly unknown. Utilizing these data for diagnose of failure is a real challenge.

Intelligent fault diagnosis automatically recognizes incipient failure which requires less prior knowledge regarding the system and requires less man-interruption during the data analysis. Supported by the Swedish transport administration (Trafikverket), we undertook a research project using Support Vector Machine (SVM) for this objective. We found SVM has an excellent theoretical foundation and it can be applied to solve real engineering problems.

SVM is an artificial intelligence technique which can automatically learn from data. SVM has intelligence or self-learning ability, and it can evolve its behavior to adapt to the new situation. This is why SVM is known to be intelligent with learning ability. SVM can be used for classification, regression, principle component analysis and so on. Figure 1 demonstrates how the SVM accommodates to the new situations, when it is used as a classifier.

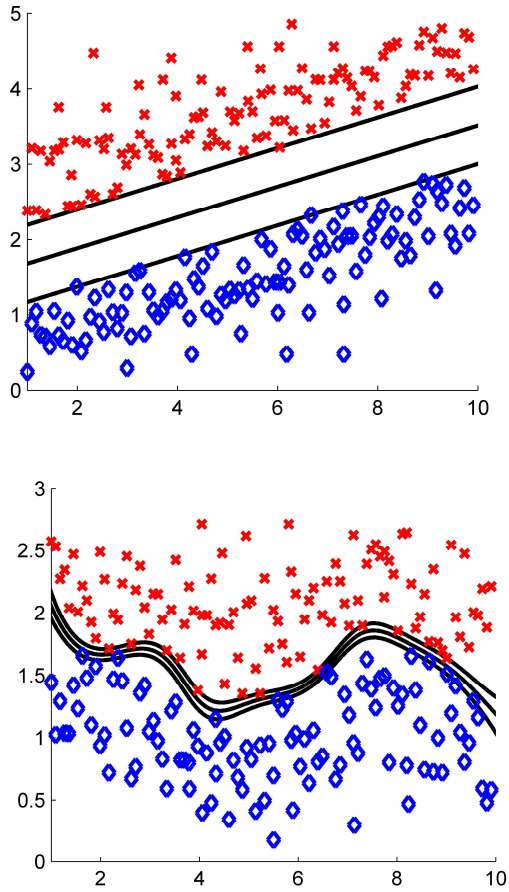



Figure 1: The red and blue dots denoting failure and health patterns of the system respectively, the black solid line is the decision function. Obviously, the decision function can adapt itself, from linear (left figure) to nonlinear (right figure), to fit the new situation, so that the two patterns can be separated.

### Comparison with Neural Network

Artificial Neural Network (ANN) is another popular technique that can be used for the intelligent failure diagnosis. From our comparative study, for middle scale data sets, whose size ranging from 50 to 300, the SVM shows a better accuracy than the classical back-propagation ANN, where the number of neurons in the hidden layer is evolutionary. As we know, the computational efficiency of learning algorithm depends on the specific training algorithm used. In this case, the SVM using active-set method to find the optimal solution is slightly efficient than classical BP ANN when the classical Levenberg-Marquardt (LM) algorithm is used to train the ANN. Table 1 shows the results from the comparative study. For this case, in terms of computational efficiency, accuracy and performance stability, the SVM can outperform the ANNs where several training algorithms are used.

Table 1. Accuracy of various learning algorithms

| Algorithms | Mean Accuracy (100%) | Max Accuracy (100%) | Min Accuracy (100%) | Mean Time Elapsed |
|---|---|---|---|---|
| SCG | 92.4 | 100 | 88 | 0.60 |
| LM | 79.6 | 100 | 20 | 0.19 |
| BFGS | 76.9 | 100 | 20 | 0.41 |
| BR | 99.2 | 100 | 97 | 0.37 |
| SVM | 100 | 100 | 100 | 0.096 |

Note: SCG-Scaled Conjugate Gradient. LM-

Levenberg - Marquardt. BFGS - BFGS quasi-Newton method. BR-Bayesian Regularized ANN.

**A Case Study**

For intelligent failure diagnosis, we have used the SVM to discriminate the inner defect bearing from the normal bearing. The left figure below is the vibration signal obtained from a test rig. After signal processing, we extracted three statistical features: impulse factor, Kurtosis and normal negative likelihood. These features are used as the input of SVM, i.e. the failure and normal pattern are represented by these three features. The linear SVM is selected for this case. Linear SVM has a decision function that is a plane in 3-dimention as shown in the right of Figure 2. This figure shows that the linear SVM can separate these patterns completely, which means the linear SVM can discriminate the inner defect bearing from normal bearing in this case.

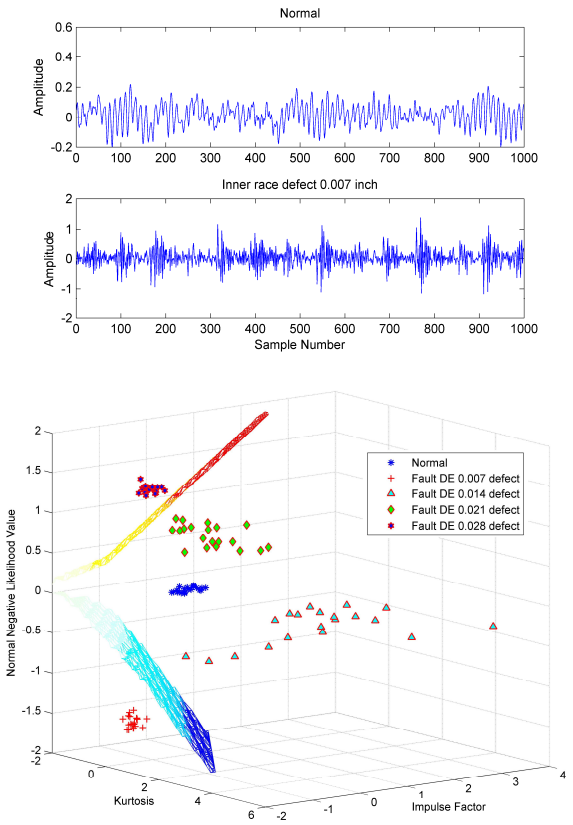



Figure 2: Vibration signal from bearing where SVM is used as a classifier.

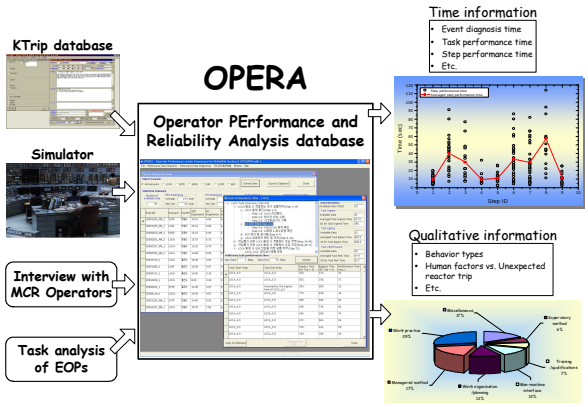
The outstanding strength of SVM for engineering application is its excellent adaptability (self-learning ability). However, for failure diagnosis, the success of SVM also critically depends on the input for the SVM. Selecting a set of proper features could improve the diagnostics accuracy significantly.

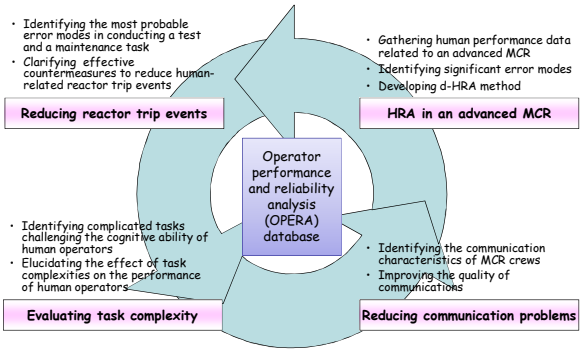
The research work reported has been performed with financial support of Swedish Transport Administration(Trafikverket) within the framework of R&D Program of Luleå Railway Research Center, Luleå, Sweden.

# OPERA: a database of operator performance in nuclear power plants

*Dr. Jinkyun Park*
*Integrated Safety Assessment Division*
*Korea Atomic Energy Research Institute,*
*Korea*

According to operating history, the performance of human operators is very crucial for the safety of nuclear power plants. In this regard, OPERA (Operator PErformance and Reliability Analysis) database has been developed in KAERI (Korea Atomic Energy Research Institute). The main role of OPERA database is to provide plant-specific and domain-specific human response times to HRA. And also it can be used as technical bases for human performance researches. To this end, over 130 audio-visual records for the re-training sessions of licensed main control room operators have been collected by using a full scope simulator of KSNP (Korean Standard Nuclear Power plant). Major tasks to be carried out under simulated emergency conditions and their response times were analyzed by goal-means task analysis and time-line analysis respectively. In addition, reactor trip reports for the past 30 years (Ktrip database) were reviewed.



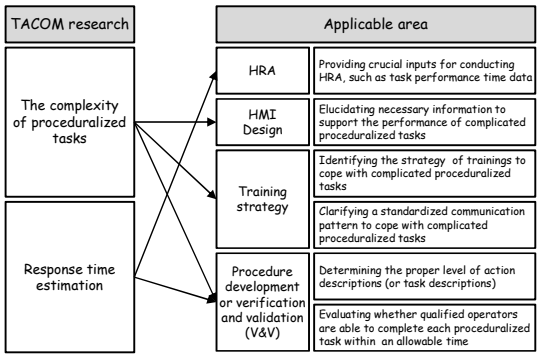



Consequently, the following results were extracted:

- Time related information;
- Dominant causes about human-related reactor trip events;
- Non-compliance behaviors in conducting procedural steps prescribed in EOPs.

Some of these results have been directly applied for HRA (human reliability analysis) purpose. For example, the response times of safety-critical tasks (HFEs; human failure events) were used to validate the appropriateness of assumptions included in HRA.

In addition, OPERA database can provide technical underpinnings for enhancing human performance. For instance, from the point of view of a good procedure development, it is very important to consider that complicated tasks are likely to impair the performance of human operators because the more the complexity increases, the more the demand of cognitive resources increases. For this reason, TAsk COMplexity (TACOM) measure has been developed to quantify the complexity of proceduralized tasks, e.g., emergency tasks stipulated in emergency operating procedures (EOPs). The comparison between TACOM scores with the associated response time data showed that there is a significant relation. This means that the following applications can be expected.




Recently, because of the introduction of a novel task environment including computerized main control rooms, the extension of OPERA database is now under consideration.

# Bayesian Integrated Reliability Analysis for Locomotive Wheels

*Jing Lin, PhD*
*Senior Researcher*
*Luleå University of Technology*
*Sweden*

Currently, the railway industry does not have a flexible decision support strategy for maintenance strategies optimization due to three defects in reliability studies: 1) Small sample data for analysis;2) Incomplete data set;3) Complex operational environments. This study aims to develop new models for integrated reliability analysis, by which to support decision making on maintenance strategies optimization. So far, both parametric Bayesian models (see Part A) and semi-parametric models (see Part B) considering frailty factors have been developed. Case studies on locomotive wheels reliability studies were performed within the framework of R&D program of Luleå Railway Research Center (JVTC) and financially supported by Swedish Transport Administration (Trafikverket), and a leading Iron Ore company LKAB which owns and maintains its own fleet of trains used for ore transport. A comparison study was also performed (see Part C). In addition, an integrated Procedure for Bayesian reliability analysis with MCMC methods is developed (see Part D) in this study.

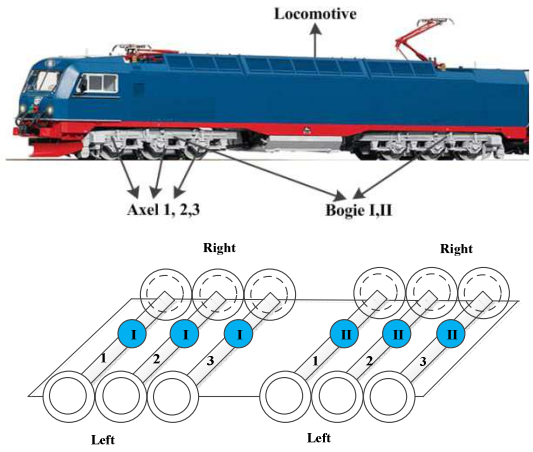



Fig. 1 Wheel positions specified in this study

Details include three parts: A, B, C, and D:

**Part A**

In parametric models' development, we have undertaken a reliability study using a Bayesian survival analysis framework (see Part D) to explore the impact of a locomotive wheel's installed position on its service lifetime and to predict its reliability

characteristics. The Bayesian Exponential Regression Model, Bayesian Weibull Regression Model and Bayesian Log-normal Regression Model are used to establish the lifetime of locomotive wheels using degradation data and taking into account the position of the wheel. This position is described by three different discrete covariates: the bogie, the axle and the side of the locomotive where the wheel is mounted. The goal is to determine reliability, failure distribution, and optimal maintenance strategies for the wheel. The results show that: 1) under specified assumptions and a given topography, the position of the locomotive wheel could influence its reliability and lifetime; 2) the Bayesian Lognormal Regression Model is a useful tool.

**Part B**

In semi-parametric models' development, we have considered the frailties simultaneously. The case study has undertaken a reliability study using a Bayesian semi-parametric framework to explore the impact of a locomotive wheel's position on its service lifetime and to predict its other reliability characteristics. A piecewise constant hazard regression model is used to establish the lifetime of locomotive wheels using degradation data and taking into account the wheel's bogie. The gamma frailties are included in this study to explore unobserved covariates within the same group. The goal is to flexibly determine reliability for the wheel. The case study is performed using Markov Chain Monte Carlo (MCMC) methods; the results show that: 1) a polynomial degradation path is a better choice for the studied locomotive wheels; 2) under given operation conditions, the position of the locomotive wheel, i.e., in which bogie it is mounted, could influence its reliability; 3) the piecewise constant hazard regression model is a useful tool since it contains fewer assumptions; 4) considering gamma frailties is helpful for exploring unobserved covariates' influence and for improving the model's precision; 5) some change points exist after the wheels run a certain distance, a finding which could be applied maintenance review and optimization.

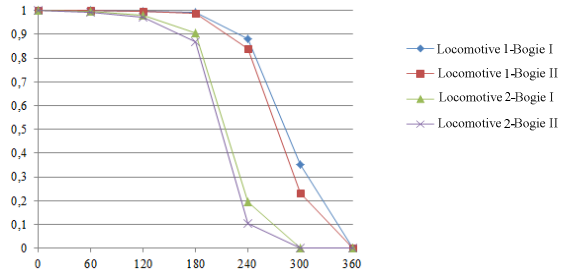
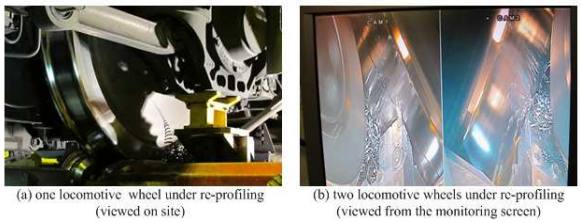



Fig.2 Plot of the reliabilities for Locomotive 1 and Locomotive 2

**Part C**

In the comparison study, we have compared the wheels on two selected locomotives on the Iron Ore Line in northern Sweden to explore some of these differences. It proposes integrating reliability assessment data with both degradation data and re-profiling performance data. Its case study compares: 1) degradation analysis using a Weibull frailty model; 2) work orders for re-profiling; 3) the performance of re-profiling parameter; and 4) wear rates. The results show that for the two locomotives: 1) under the specified installation position and operation conditions, the Weibull frailty model is a useful tool to determine wheel reliability; 2) rolling contact fatigue (RCF) is the principal reason for re-profiling work orders; 3) the re-profiling parameters can be applied to monitor both the wear rate and the re-profiling loss; 4) the total wear of the wheels can be investigated by considering natural wear and re-profiling loss separately, but natural wear and re-profiling loss differ depending on the locomotive and the operating conditions; and 5) the bogie in which a wheel is installed influences wheel reliability.


(a) one locomotive wheel under re-profiling (viewed on site)

(b) two locomotive wheels under re-profiling (viewed from the monitoring screen)

Fig. 3 Locomotive wheels on-site re-profiling

**Part D**

The advent of Markov Chain Monte Carlo (MCMC) approaches have proliferated Bayesian inference in a wide variety of fields. In order to facilitate their applications, this study proposes an integrated procedure for Bayesian inference via MCMC methods, from a reliability perspective. The goal is to build a full framework for related academic research and engineering applications with respective to implementing modern computational-based Bayesian approaches, especially to reliability inference.

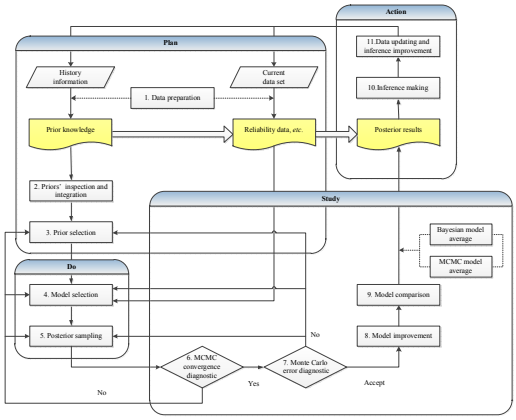



*Fig.4 An Integrated Procedure for Bayesian Reliability Inference via MCMC*

The proposed procedure is considered as a continuous improvement process with four stages (Plan, Do,

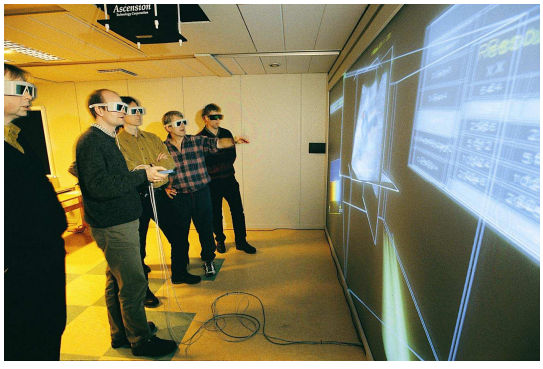
Study, and Action) and eleven steps from a step-by-step point of view, including: 1) Data preparation; 2) Priors' inspection and integration; 3) Prior selection; 4) Model selection; 5) Posterior sampling; 6) MCMC convergence diagnostic; 7) Monte Carlo error diagnostic; 8) Model improvement; 9) Model comparison; 10) Inference making; 11) Data updating and inference improvement. Relevant discussions support the conclusion that, the integrated procedure is a useful tool.

The results reported here are a part of research report submitted to Luleå railway Research Center.

## A new European funded project TOSCA

*Zoe Nivolianitou*
*Demokritos Institute, Greece*

A new European funded project **TOSCA (**Total Operations Management for Safety Critical Activities) has been aviated on February 1st, 2013. TOSCA is concerned with the integration of industrial operations into a total performance management system. Within TOSCA safety, quality and productivity are addressed in an integrated way during the lifecycle of projects or products. TOSCA's industrial domain of application concerns process control industries (e.g., chemical industries, power generation, offshore oil & gas platforms, etc.) that may vary in size, regulatory and cultural aspects. TOSCA will examine vulnerabilities of the technical, human and organizational systems that may have an impact in safety, quality and productivity. Safety of critical activities can be seen as 'projects' or 'safety cases' that must be examined from the perspectives of many stakeholders (e.g., different departments, subcontractors, regulatory authorities, etc.) and decision-making at different organizational levels (e.g. top managers, supervisors and operators).



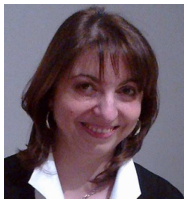
A participative approach will be applied that should collect knowledge from the sharp-end operators and integrate it with formal descriptions of system operation and response. Furthermore, TOSCA will enhance the management of change and provide an environment for testing out the effectiveness of possible action plans.

Project coordinator is the engineering-consultancy firm DAPPOLONIA in Italy, while members come from all over Europe, namely: Celtic Oil, Reviatech, Trinity College Dublin, NCSR "Demokritos", Institut National de l'Environnement Industriel et des Risques, Jožef Stefan Institute, Politecnico di Torino, Technical University of Crete and University of Bologna. As end users participate the companies: K&N Efthimiades Agrochemicals, Plinarna Maribor LPG plant., Electricity Supply Board International, UEAPME and PROMIS.

The project is funded under the SEVENTH FRAMEWORK PROGRAMME (FP7-NMP-2012-SMALL-6) of the EC, as a Collaborative Project of small or medium scale and will conclude its works within three years from start up. Dr. Keith Simons has been appointed as Project Technical Adviser (PTA).

# PhD Degrees Completed

## Methods for the Vulnerability Analysis of Critical Infrastructures



*Roberta Piccinelli*
*Supervisor :*
*Prof. Enrico Zio*
*Co-supervisor:*
*Dr. Giovanni Sansavini*

The subject of this PhD thesis concerns methods for the analysis of critical infrastructures with respect to their vulnerabilities to random failures and targeted attacks. The work has been performed at the Laboratorio di Analisi di Segnale ed Analisi di Rischio (LASAR Laboratory of Signal Analysis and Risk Analysis) of the Department of Energy of the Politecnico di Milano.

Critical infrastructures (CIs) are large scale, spatially distributed, engineered complex systems which provide vital services for modern society, such as energy supply (electricity, oil and gas supply), transportation (by rail, road, air, shipping), information and telecommunication (such as the internet), drinking water distribution, including wastewater treatment.

Outages or mishaps in CIs cause disruption or incapacitation of fundamental services and result in diverse consequences with economical and social implications.

For this reason, a comprehensive vulnerability analysis of CIs requires not only identifying the logical and functional relationships among the large number of spatially distributed, interacting elements but also accounting for a broad spectrum of hazards and threats including random failures and intentional attacks.

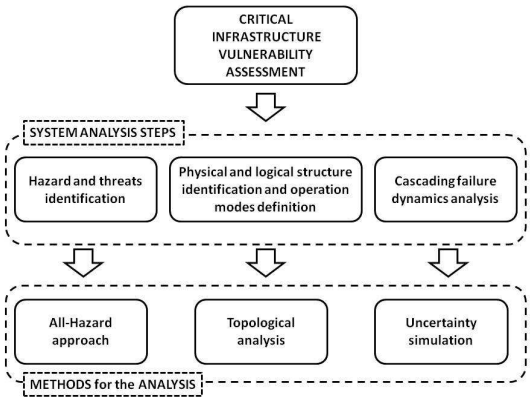



Figure 1. Pictorial view of the critical infrastructure vulnerability assessment presented in the present PhD thesis

The conceptualization of critical infrastructure vulnerability assessment implies system analysis for (figure 1):

a. hazards and threats identification;
b. physical and logical structure identification and operational modes definition;
c. cascading failure dynamics analysis.

In this thesis, three methods for the analysis have been devised to perform the vulnerability analysis:

- the all-hazard approach to address issue a;
- the topological analysis to address issue b;
- uncertainties analysis to address issue c.

CIs are especially attractive targets for malevolent attacks because today's societies operate heavily on their reliance. In risk and vulnerability analysis, random accidents, natural failures and unintentional man-made hazards are typically known and categorized by emergency planners. The likelihood of their occurrence is traditionally addressed within a probabilistic framework. On the other hand, terrorism poses a hazard that eludes a quantification by probability theory due to the intentional and malevolent planning it implies. Therefore, there is the need of an all–hazard approach encompassing a broader view on the hazards, that threaten CIs. The all-hazard approach is intended to provide the basis for addressing unexpected events of any nature such as deterioration and random failures, natural disasters, accidents, and malevolent acts. In this PhD thesis, an *All-HAZard ANalysis* (A-HAZAN) is developed. It aims at identifying the features, operating conditions and failure modes relevant to CI vulnerability, and capturing the CIs vulnerability sources and issues, given their technical and physical features, and the dependencies and interdependencies on other CIs.

CIs are engineered complex systems and can be modelled as hierarchies of interacting components. In this view, the actual structure of the network of interconnections among the components is a critical feature of the system. In a topological analysis, a CI is represented by a graph *G(N, K)*, in which its physical constituents (components) are mapped into *N* nodes (or vertices) connected by *K* edges (or arcs), representing the links of physical connections among them. The focus of topological analysis is on the structural properties of the graphs. In order to quantify the structural importance of the network components, several centrality measures have been introduced: commonly used centrality measures identify the most important elements in networks of components, based on the assumption that physical/communication/service among nodes flow follows the shortest paths in the network. In spite of the usefulness and appealing simplicity of the topological analysis of the network underpinning a CI and of the insights it provides, empirical results show that it cannot capture the rich and complex properties observed in a real infrastructure system, so that there is a need for extending the models beyond pure structural topology. While the topological approaches for identifying critical components are capable of highlighting structural vulnerabilities, they are limited from the point of view of the functional vulnerability of the CI. In real network systems, another important dimension to add to the vulnerability characterization refers to modelling the dynamics of flow of the physical quantities in the network where physical law and operational rules drive the physical/communication/service flow. This entails considering the interplay between structural characteristics and the dynamics, in order to provide indications on the elements critical for the propagation process and on the actions that can be performed in order to prevent or mitigate the undesired effects.

In the final step of the CI vulnerability analysis developed in this PhD thesis, the characterization of uncertainties related to the physical flow through the network has been undertaken and exemplified with respect to the electric infrastructure. Failing to incorporate uncertainties in system planning may lead to an overestimation of risk reduction barriers and of system capabilities to maintain acceptable levels of reliability. In order to quantify the impact that the propagation of the identified uncertainties has on the reliability of the electric infrastructure a stochastic model that simulates the operations of an electric transmission network was developed. This event based model, embedded in the Monte Carlo Simulation framework, and has shown the ability to represent daily hourly changes in power requests at customer side of the system, ambient temperature, wind speed and wind power generation. The increasing variability in the operating conditions lead to an increase in the generated power that cannot be supplied to the customers.

# Calendar of Safety and Reliability Events

## 22nd SRA-European Annual Conference

Trondheim, Norway
17 - 19 June 2013

The theme of the conference is "Safe societies – coping with complexity and major risk", concerning challenges related to our society's vulnerability to major risk of natural and industrial disasters, malicious attacks, financial breakdowns and epidemic diseases.

The conference is open to all interested researchers, experts and industry representatives interested in risk analysis, including risk assessment, characterization, communication, management, and policy across all sectors and societal levels.

Important dates

**15 January, 2013** - Deadline for submission of abstract and symposia.
**1 June, 2013** - Deadline for submission of optional full length papers.
Conference Website: www.srae2013.no

## 2nd International Conference on Transportation Information and Safety - ICTIS 2013

Wuhan, China, 28 June - 1 July

Conference Website: www.ictis-online.org:8080/ictis

## 8th International Conference on Mathematical Methods in Reliability: Theory, Methods, and Applications - MMR2013

Stellenbosch, South Africa, 1-4 July

The theme of MMR 2013 is "Reliability: A View of the Past and Ideas for the Future". It aims at enhancing international exchanges and promoting advances in reliability/risk theories and techniques, and organizing an international forum on emerging issues in reliability engineering and risk management. We sincerely hope that you can join us for a rich experience in this unique environment.

Conference Website: www.sastat.org.za/mmr2013

## 4th International Conference on Risk Analysis and Crisis Response (RACR 2013)

Istanbul, Turkey, 27-29 August

Important dates

| Deadline | Notification |
|---|---|
| Special session proposals | 1 December 2012<br>1 January 2013 |
| Abstract submission | 1 February 2013<br>15 February 2013 |
| Paper submission | 1 April 2013<br>15 April 2013 |
| Final paper due | 1 May 2013 |

Contact

Prof. Dr. Cengiz KAHRAMAN
Chairman, Program Committee of RACR2013
Istanbul Technical University
Department of Industrial Engineering
34367 Macka Istanbul, TURKEY
Tel : +90-212-2931300 Ext. 2035
Fax : +90-212-2407260
E-mail: kahramanc@itu.edu.tr

Conference Website: www.flins2012.itu.edu.tr

## 2013 Prognostics and System Health Management Conference - PHM 2013

Milan, Italy, 8-11 September 2013

Presentation of developments in various industrial fields is expected to highlight differences in research challenges and practical needs, while at the same time beneficiating from cross-fertilization of methods and applications.

The event is organized by AIDIC, The Italian Association of Chemical Engineering.

Details on the Conference may be found at http://www.aidic.it/phm>www.aidic.it/phm

The First Deadline for Abstract Submission is: **23 October, 2012**

Submission of abstracts can be done electronically at

http://www.aidic.it/phm/abstractsubmission.html>http://www.aidic.it/phm/abstractsubmission.html

Accepted papers presented during the Conference will be published in Chemical Engineering Transactions http://www.aidic.it/cet>http://www.aidic.it/cet. The quality of this publication is valued by ISBN & ISSN numbers, referenced by SCOPUS and THOMSON REUTERS (ISI Web of Knowledge, conference proceedings) indexes.

Also, the extended version of selected papers presented at the Conference will be proposed for special issues on indexed scientific journals.

For any further information or assistance you may contact the secretariat at phm@aidic.it.

Important dates

**October 23, 2012 -** Abstract Submission
**November 23, 2012 -** Abstract Acceptance

**January 23, 2013 -** Full Paper Submission
**March 23, 2013** - Notification of Acceptance/Rejection
**April 3, 2013** - Notification of lecture/poster presentation
**May 23, 2013** - Final revised manuscript submission and Registration deadline for Authors to have the paper included in final program and proceedings

Secretariat

Correspondence should be addressed to AIDIC Secretariat:
**PHM-2013 Secretariat**
c/o AIDIC – The Italian Association of Chemical Engineering
Attn. Raffaella DAMERIO
Via Giuseppe Colombo 81/A - 20133 Milano (Italy)
Tel: +39-02-70608276; Fax: +39-02-70639402; e-mail: phm@aidic.it
Conference Website: www.aidic.it/phm

## 11th International Probabilistic Workshop

Brno, Czech Republic
6 - 8 November 2013

The conference is intended for civil and structural engineers and other professionals concerned with structures, systems or facilities that require the assessment of safety, risk and reliability. Participants could therefore be consultants, contractors, suppliers, owners, operators, insurance experts, authorities and those involved in research and teaching.

Contact

Drahomír Novák and Miroslav Vorechovský
Brno University of Technology (BUT)
Faculty of Civil Engineering
Institute of Structural Mechanics
Czech Republic
Veverí 95, 602 00 Brno
Czech Republic
Tel: +420 541 147 360
Fax: +420 541 240 994
Email: ipw11@fce.vutbr.cz

Dirk Proske
University of Natural Resources and Applied Life Sciences, Vienna
Institute for Mountain Risk Engineering
Peter Jordan-Street 82
1190 Wien, Austria
Email: dirk.proske@boku.ac.at

Conference Website: http://ipw11.fce.vutbr.cz/

# ESRA Information

### 1 ESRA Membership

### 1.1 National Chapters

- French Chapter
- German Chapter
- Italian Chapter
- Polish Chapter
- Portuguese Chapter
- Spanish Chapter
- UK Chapter

### 1.2 Professional Associations

- The Safety and Reliability Society, UK
- Danish Society of Risk Assessment, Denmark
- SRE Scandinavia Reliability Engineers, Denmark
- ESReDA, France
- French Institute for Mastering Risk (IMdR-SdF), France
- VDI-Verein Deutscher Ingenieure (ESRA Germany), Germany
- The Netherlands Society for Risk Analysis and Reliability (NVRB), The Netherlands
- Polish Safety & Reliability Association, Poland
- Asociación Española para la Calidad, Spain

### 1.3 Companies

- TAMROCK Voest Alpine, Austria
- IDA Kobenhavn, Denmark
- VTT Industrial Systems, Finland
- Bureau Veritas, France
- INRS, France
- Total, France
- Commissariat á l'Energie Atomique, France
- DNV, France
- Eurocopter Deutschland GMbH, Germany
- GRS, Germany
- SICURO, Greece
- VEIKI Inst. Electric Power Res. Co., Hungary
- Autostrade, S.p.A, Italy
- D'Appolonia, S.p.A, Italy
- IB Informatica, Italy
- RINA, Italy
- TECSA, SpA, Italy
- TNO Defence Research, The Netherlands
- Dovre Safetec Nordic AS, Norway
- PRIO, Norway
- SINTEF Industrial Management, Norway
- Central Mining Institute, Poland
- Adubos de Portugal, Portugal
- Transgás - Sociedade Portuguesa de Gás Natural, Portugal
- Cia. Portuguesa de Producção Electrica, Portugal
- Siemens SA Power, Portugal
- ESM Res. Inst. Safety & Human Factors, Spain
- IDEKO Technology Centre, Spain
- TECNUN, Spain
- TEKNIKER, Spain
- CSIC, Spain
- HSE - Health & Safety Executive, UK
- Atkins Rails, UK
- W.S. Atkins, UK
- Railway Safety, UK
- Vega Systems, UK

### 1.4 Educational and Research Institutions

- University of Innsbruck, Austria
- University of Natural Resources & Applied Life Sciences, Austria
- AIT Austrian Institute of Techn. GmbH, Austria
- Université Libre de Bruxelles, Belgium
- University of Mining and Geology, Bulgaria
- Czech Technical Univ. in Prague, Czech Republic
- Technical University of Ostrava, Czech Republic
- Technical University of Liberec, Czech Republic
- University of Defence, Czech Republic
- Tallin Technical University, Estonia
- Helsinki University of Technology, Finland
- École de Mines de Nantes, France
- Université Henri Poincaré (UHP), France
- Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS), France
- Université de Bordeaux, France
- Université de Technologie de Troyes, France
- Université de Marne-la-Vallée, France
- INERIS, France
- Fern University, Germany
- Technische Universität Muenchen, Germany
- Technische Universität Wuppertal, Germany
- University of Kassel, Germany
- TU Braunschweig, Germany
- Institute of Nuclear Technology Radiation Protection, Greece
- University of the Aegean, Greece
- Universita di Bologna (DICMA), Italy
- Politecnico di Milano, Italy
- Politecnico di Torino, Italy
- University of Rome "La Sapiensa", Italy
- Universita Degli Studi di Pavia, Italy
- Universita Degli Studi di Pisa, Italy
- Technical University of Delft, The Netherlands
- Institute for Energy Technology, Norway
- Norwegian Univ. Science & Technology, Norway
- University of Stavanger, Norway
- Technical University of Gdansk, Poland
- Gdynia Maritime Academy, Poland
- Institute of Fundamental Techn. Research, Poland
- Technical University of Wroclaw, Poland
- Instituto Superior Técnico, Portugal
- Universidade de Coimbra, Portugal
- Universidade Nova de Lisboa - FCT, Portugal
- Universidade de Minho, Portugal
- Universidade do Porto, Portugal
- University Politechnica of Bucharest, Romania
- University of Iasi, Romania
- Slovak Academy of Sciences, Slovakia
- University of Trencin, Slovakia
- Institute "Jozef Stefan", Slovenia
- Asociación Española para la Calidad, Spain
- PMM Institute for Learning, Spain
- Universidad D. Carlos III de Madrid, Spain
- Universidad de Extremadura, Spain
- Univ. de Las Palmas de Gran Canaria, Spain
- Universidad Politecnica de Madrid, Spain
- Universidad Politecnica de Valencia, Spain
- Institute de Matematica y Fisica Fundamental (IMAFF), Spain
- University of Castilla-La Mancha, Spain
- LuleåUniversity, Sweden
- World Maritime University, Sweden
- Institut f. Energietechnik (ETH), Switzerland
- Paul Scherrer Institut, Switzerland
- City University London, UK
- Liverpool John Moores University, UK
- University of Aberdeen, UK
- University of Bradford, UK
- University of Salford, UK
- University of Strathclyde, Scotland, UK

### 1.5 Associate Members

- Federal University of Pernambuco, Brazil
- Fluminense Federal University, Brazil
- Pontifícia Universidade Católica, Brazil
- Universidad Central de Venezuela, Venezuela
- European Commission - DR TREN (Transport and Energy), in Luxembourg
- Vestel Electronics Co., Turkey

## 2 ESRA Officers

### Chairman

Enrico Zio (enrico.zio@polimi.it)
Politecnico di Milano, Italy
Ecole Centrale Paris, Supelec

### Vice-Chairman

Terje Aven (terje.aven@uis.no)
University of Stavanger, Norway

### General Secretary

Coen van Gulijk (c.vangulijk@tudelft.nl)
Delft University of Technology, The Netherlands

### Treasurer

Radim Bris (radim.bris@vsb.cz)
Technical University of Ostrava, Czech Republic

### Past Chairman

Ioannis Papazoglou (yannisp@ipta.demokritos.gr)
NCSR Demokritos Institute, Greece

### Chairmen of the Standing Committees

K. Kolowrocki, Gdynia Maritime University, Poland
C. Guedes Soares, Instituto Superior Técnico, Portugal

## 3 Management Board

The Management Board is composed of the ESRA Officers plus one member from each country, elected by the direct members that constitute the National Chapters.

## 4 Standing Committees

### 4.1 Conference Standing Committee

Chairman: K. Kolowrocki, Gdynia Maritime Univ., Poland

The aim of this committee is to establish the general policy and format for the ESREL Conferences, building on the experience of past conferences, and to support the preparation of ongoing conferences. The members are one leading organiser in each of the ESREL Conferences.

### 4.2 Publications Standing Committee

Chairman: C. Guedes Soares, Instituto Sup. Técnico, Portugal

This committee has the responsibility of interfacing with Publishers for the publication of Conference and Workshop proceedings, of interfacing with Reliability Engineering and System Safety, the ESRA Technical Journal, and of producing the ESRA Newsletter.

## 5 Technical Committees

**Technological Sectors**

### 5.1 Aeronautics Aerospace

Chairman: Darren Prescott, UK
E-mail: d.r.prescott@lboro.ac.uk

**5.2 Critical Infrastructures**
Chairman: W. Kröger, Switzerland
E-mail: kroeger@mavt.ethz.ch

**5.3 Energy**
Chairman: Kurt Petersen, Sweden
E-mail: Kurt.Petersen@lucram.lu.se

**5.4 Information Technology and Telecommunications**
Chairman: Elena Zaitseva, Slovakia
E-mail: Elena.Zaitseva@fri.uniza.sk

**5.5 Manufacturing**
Chairman: Benoit Lung, France
E-mail: Benoit.Iung@cran.uhp-nancy.fr

**5.6 Nuclear Industry**
Chairman: S. Martorell, Univ. Poli. Valencia, Spain
E-mail: smartore@iqn.upv.es

**5.7 Safety in the Chemical Industry**
Chairman: M. Christou, Joint Research Centre, Italy
Email: Michalis.Christou@jrc.ec.europa.eu

**5.8 Land Transportation**
Chairman: Valerio Cozzani, Italy
E-mail: valerio.cozzani@unibo.it

**5.9 Maritime Transportation**
Chairman: Jin Wang, UK
E-mail: J.Wang@ljmu.ac.uk

**5.10 Natural Hazards**
Chairman: P. van Gelder, The Netherlands
Email: p.h.a.j.m.vangelder@tudelft.nl

**Methodologies**

**5.11 Accident and Incident Modelling**
Chairman: Stig O. Johnson, Norway
Email: stig.o.johnsen@sintef.no

**5.12 Prognostics & System Health Management**
Chairman:Piero Baraldi, Italy
E-mail: Piero.baraldi@polimi.it

**5.13 Human Factors and Human Reliability**
Chairman: Luca Podofillini, Switzerland
Email: Luca.podofillini@psi.ch

**5.14 Maintenance Modelling and Applications**
Chairman: Christophe Bérenguer, France
Email: christophe.berenguer@utt.fr

**5.15 Mathematical Methods in Reliability and Safety**
Chairman: John Andrews, UK
Email: John.Andrews@nottingham.ac.uk

**5.16 Quantitative Risk Assessment**
Chairman: Marko Cepin, Slovenia
E-mail: marko.cepin@fe.uni-lj.si

**5.17 Systems Reliability**
Chairman: Gregory Levitin, Israel,
E-mail: levitin@iec.co.il

**5.18 Uncertainty Analysis**
Chairman: Emanuele Borgonovo, Italy,
E-mail: emanuele.borgonovo@unibocconi.it

**5.19 Safety in Civil Engineering**
Chairman: Raphael Steenbergen, The Netherlands
Email: Raphael.steenbergen@tno.nl

**5.20 Structural Reliability**
Chairman: Jana Markova, Czech Republic
E-mail: Jana.Markova@klok.cvut.cz

**5.21 Occupational Safety**
Chairman: Ben Ale, The Netherlands
Email: B.J.M.Ale@tudelft.nl

ESRA is a non-profit international organization for the advance and application of safety and reliability technology in all areas of human endeavour. It is an "umbrella" organization with a membership consisting of national societies, industrial organizations and higher education institutions. The common interest is safety and reliability.
For more information about ESRA, visit our web page at http://www.esrahomepage.org.
For application for membership of ESRA, please contact the general secretary Coen van Gulijk E-mail: C.vanGulijk@tudelft.nl.
Please submit information to the ESRA Newsletter to any member of the Editorial Board: